

RICHTLINIEN

FÜR DEN

DATENSCHUTZKONFORMEN EINSATZ

DES PRODUKTS

KASEYA IT AUTOMATION FRAMEWORK

AUTOR:

PROF. DR. RAINALD SCHÖNEBERG
LEHRGEBIET WIRTSCHAFTSINFORMATIK
FACHBEREICH TECHNISCHE BETRIEBSWIRTSCHAFT
FACHHOCHSCHULE SÜDWESTFALEN



INHALT


Fachhochschule
Südwestfalen
University of Applied Sciences

ABKÜRZUNGSVERZEICHNIS

AD	Active Directory
ADV	Auftragsdatenverarbeitung (im Sinne des § 11 BDSG)
AES	Advanced Encryption Standard (Blockverschlüsselung)
ASP	Active Server Pages
BfDI	Der Bundesbeauftragte für Datenschutz und Informationssicherheit
BDSG	Bundesdatenschutzgesetz
DVA	Datenverarbeitung im Auftrag
EU	Europäische Union
EWR	Europäischer Wirtschaftsraum
FTP	File Transfer Protocol
Guid	Globally Unique Identifier
IIS	Internet Information Services
KLC	Kaseya Live Connect
KunstUrhG	Kunsturhebergesetz
KServer	Kaseya Server VSA
ML	Managed Location
MSE	Managed Services Edition
MSP	Managed Service Provider
PBD	Personenbezogene Daten
RC4	„Ron’s code 4“ (Stromverschlüsselung von Ronald L. Rivest)
RFP	Remote Framebuffer Protocol
SHA	Secure Hash Algorithm
StGB	Strafgesetzbuch
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
VNC	Virtual Network Computing
VSA	Virtual System Administrator
WSDL	Web Services Description Language

ABBILDUNGSVERZEICHNIS

TABELLENVERZEICHNIS



ZUSAMMENFASSUNG

Das ***Kaseya IT Automation Framework*** unterstützt effektiv und effizient jedes automatisierte Verfahren, bei dem ein Auftragnehmer die Fernwartung/Fernbetreuung von IT-Infrastrukturen eines Auftraggebers durchführt. Da dabei - insbesondere bei den Geschäftsprozessen der Fernwartung - auch personenbezogene Daten im Sinne des Bundesdatenschutzgesetzes (BDSG) erhoben und verwendet werden, sind beim Einsatz des *Kaseya IT Automation Framework* die einschlägigen Vorschriften des Datenschutzrechts zu beachten.

Die in diesem Dokument beschriebene Untersuchung der Datenschutzkonformität des *Kaseya IT Automation Framework* ergab, dass eine **sehr hohe, überwiegend sogar vorbildliche Datenschutzkonformität** durch die in diesem Gutachten identifizierten Empfehlungen zur Administration, zur Installation und zur Konfiguration des *Kaseya IT Automation Framework* sichergestellt werden kann.

Wesentliche administrative Empfehlungen sind:

1. ein angemessenes Datenschutzniveau des Auftraggebers, insbesondere hinsichtlich personenbezogener Daten, die sich auf den ferngewarteten Rechnern befinden,

2. ein angemessenes Datenschutzniveau des Auftragnehmers,

3. eine besondere Eignung des Auftragnehmers für die Fernwartung/Fernbetreuung auf Basis des *Kaseya IT Automation Framework*,

4. die Gestaltung des Vertrags zwischen Auftraggeber und Auftragnehmer entsprechend § 11 BDSG und die präzise Einhaltung der Vorschriften dieses Vertrages,

5. die Bestellung eines Datenschutzbeauftragten entsprechend § 4f, § 4g BDSG beim Auftragnehmer,

6. die Einholung informierter Einwilligungen entsprechend § 4a BDSG für den Einsatz des *Kaseya IT Automation Framework* von allen Personen, die einen ferngewarteten Rechner beim Auftraggeber benutzen,

7. die Einholung informierter Einwilligungen entsprechend § 4a BDSG von allen Benutzern des Webportals des *Kaseya IT Automation Framework*,

8. die schriftliche Verpflichtung der beteiligten Mitarbeiter des Auftragsnehmers auf das Datenschutzgeheimnis entsprechend § 5 BDSG und

9. die schriftliche Verpflichtung der beteiligten Mitarbeiter des Auftragnehmers, personenbezogene Daten, die ihnen im Rahmen der Erfüllung dieses Vertrags bekannt werden, nur für Zwecke der Fernwartung/Fernbetreuung gemäß diesem Vertrag zu verwenden und - wenn möglich - auf eine Verwendung gänzlich zu verzichten.

Wesentliche Empfehlungen zur Installation und zur Konfiguration sind:

1. den Kaseya Agent sowie Software für Fernzugriffe, Dateiübertragungen und Chats voll transparent für die Person, die den ferngewarteten Rechner benutzt, zu installieren und zu betreiben,

2. eine aussagekräftige Datenschutzerklärung in den Kaseya Agent zu integrieren, die die Person, die einen ferngewarteten Rechner benutzt, jederzeit abrufen kann,

3. jeder Person, die einen ferngewarteten Rechner benutzt, über einen Zugriff zum Webportal des *Kaseya IT Automation Framework* jederzeit Einblick in alle über diesen Rechner und über seine Person gespeicherten Daten zu ermöglichen,

4. keine Fernzugriffe oder Dateiübertragungen ohne (elektronische) Genehmigung der Person, die den ferngewarteten Rechner gegenwärtig benutzt, durchzuführen,

5. alle bei Fernzugriffen, Dateiübertragungen und Chats anfallenden Datenübertragungen von und zu einem ferngewarteten Rechner mit dem Advanced Encryption Standard (AES) zu verschlüsseln,

6. den gesamten Email-Verkehr, der im Zuge der Durchführung der Fernwartung und Fernbetreuung entsteht, wirksam gegen unbefugte Einsichtnahme zu schützen (etwa durch den Einsatz von SSL),

7. den Server und das Webportal des *Kaseya IT Automation Framework* auf einem dedizierten Rechner zu betreiben, der - entsprechend der Anzahl der ferngewarteten Rechner - die vom Hersteller empfohlene Ausstattung aufweist,

8. das Webportal des *Kaseya IT Automation Framework* durch eine aussagekräftige Datenschutzerklärung und eine Anbieterkennzeichnung (mit Angaben zum Auftragnehmer, nicht zum Hersteller!) entsprechend den Vorschriften des Telemediengesetzes (TMG) zu ergänzen,

9. den Zugang zum Webportal des *Kaseya IT Automation Framework* nur über das Protokoll HTTPS zu ermöglichen,

10. alle Benutzerkennungen für den Zugang zum Webportal des *Kaseya IT Automation Framework* personengebunden zu vergeben und keine Sammelbenutzerkennungen zuzulassen,

11. adäquate Benutzerkennwortregeln (Mindestlänge: 8; Zeichensätze: Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen; Änderung: spätestens alle 30 Tage; Wiederholung: frühestens alle 3 Monate; Sperrung: nach 5 Fehleingaben für mindestens 1 Stunde) für den Zugang zum *Kaseya IT Automation Framework* zu erzwingen,

12. den Mitarbeitern im Hause des Auftragnehmers - mit Ausnahme von Systemadministratoren - keinen direkten Zugriff auf die zugrunde liegende Datenbank über Datenbankansichten o.ä. zu ermöglichen,

13. den Mitarbeitern im Hause des Auftragnehmers bei ihren Fernwartungs- und Fernbetreuungsaktivitäten für den Auftraggeber nur Zugriff auf die Daten dieses Auftraggebers zu ermöglichen,

14. die Löschungsfristen von Log- und Protokolldaten auf höchstens 30 Tage zu setzen (falls keine dagegen stehenden Verpflichtungen bestehen) und Archivierungen dieser Daten nicht im Webportal des *Kaseya IT Automation Framework* sondern allenfalls im Rahmen von Systemsicherungen zuzulassen.

Zudem ergaben sich im Zuge der Untersuchungen folgende **Empfehlungen an den Hersteller zur weiteren Förderung der Datenschutzkonformität**:

1. Im Agentenmenü den Punkt „About Agent“ so konfigurierbar zu machen, dass eine Datenschutzerklärung für die Personen, die den ferngewarteten Rechner benutzen, ständig verfügbar gehalten werden kann (§ 4 BDSG).

2. Re-Design der Benutzeroberfläche des Webportals des *Kaseya IT Automation Framework* so, dass eine Anbieterkennzeichnung des Diensteanbieters und eine Datenschutzerklärung für die Nutzer leicht erkennbar, unmittelbar erreichbar und ständig verfügbar gehalten werden kann (§ 5 TMG).

3. Verschlüsselung der Datenbestände des *Kaseya IT Automation Framework*, insbesondere der Datenbank (Anlage zu § 9 Satz 1 BDSG).

4. Integration von Anonymisierungs- bzw. Pseudonymisierungsfunktionen, insbesondere bei den Berichtserstellungen des *Kaseya IT Automation Framework* (§ 3a BDSG, § 15 TMG).

5. Bereinigung der Datenbank des *Kaseya IT Automation Framework* durch Entfernen unnötiger oder ungenutzter personenbezogener Datenfelder, insbesondere solcher, die besondere personenbezogene Daten repräsentieren (§ 3 (9), § 3a BDSG).

6. Anpassung der Voreinstellungen im Webportal des *Kaseya IT Automation Framework* für Benutzerkennworte an den Stand der Technik und für Log- und Protokolldateien an angemessene Aufbewahrungsfristen (§9, § 20 (2) BDSG).



HINTERGRUND

Die *Kaseya International Deutschland GmbH, Europaplatz 10, 44269 Dortmund* (nachfolgend *GmbH* genannt) vertreibt das ***Kaseya IT Automation Framework***[1], um u.a. einem Systemhaus („managed service provider“, nachfolgend MSP genannt) ein effektives und effizientes Management von (entfernten) IT-Infrastrukturen bei einem Kunden („managed location“, nachfolgend ML genannt) per Fernzugriff über eine webgestützte Plattform („Webportal“) zu ermöglichen.

Die *GmbH* will darauf hinwirken, dass der Einsatz des *Kaseya IT Automation Framework* in einem Verfahren[2] der Fernwartung/Fernbetreuung hinsichtlich Datenschutz, Datensicherheit und Gebrauchstauglichkeit stets den höchsten Ansprüchen genügt.

AUFGABENSTELLUNG

Die *GmbH* hat dementsprechend den Autor beauftragt, für den Einsatz des Produktes *Kaseya IT Automation Framework* die Anforderungen, die sich aus den geltenden Regelungen des Datenschutzes ergeben, zu benennen und Empfehlungen zu erarbeiten, die einen datenschutzkonformen Betrieb weitgehend sicherstellen. Die Datensicherheit soll dabei nur so weit berücksichtigt werden, wie es der Datenschutz verlangt.[3]

Diese Empfehlungen sollen - im Sinne von Richtlinien - Verpflichtungen, Vereinbarungen und Maßnahmen für den MSP und die ML derart beinhalten, dass Datenschutzkonformität beim Einsatz von *Kaseya IT Automation Framework* für alle Parteien entsteht, falls diese Richtlinien eingehalten werden. Dabei geht es sowohl um den Schutz der personenbezogenen Daten von Mitarbeitern, die einen ferngewarteten Rechner im Hause ML bei ihrer täglichen Arbeit einsetzen, als auch um den Schutz der personenbezogenen Daten von Mitarbeitern des MSP, die die Fernwartung/Fernbetreuung der ML durchführen. Hinzu kommen ggf. personenbezogene Daten von Geschäftspartnern der ML und von weiteren Personen, die sich möglicherweise auf den ferngewarteten Rechnern befinden.

---

[1] Im gesamten nachfolgenden Text ist eine Mischung von englischen und deutschen Bezeichnungen bzw. Beschreibungen oder die Verwendung „unglücklicher“ Übersetzungen (wie ‚Werkzeugspitze‘ für ‚Tool Tip‘ oder ‚Fenster‘ für ‚Windows‘) leider nicht vollständig vermeidbar, da auch bei Nutzung der deutschen Sprache als Voreinstellung die Version MSE K2 sowie die Dokumentationen/Hilfesysteme diese Mischung und diese Übersetzungen verwenden.

[2] Der Begriff **Verfahren** bezeichnet ein Bündel von automatisierten Verarbeitungen, die über eine definierte Zweckbindung miteinander verbunden sind. Somit kann ein Verfahren aus mehreren automatisierten Verarbeitungen und mehreren Geschäftsprozessen bestehen.

[3] Sowohl Datensicherheit als auch Gebrauchstauglichkeit (**Usability**), insbesondere Barrierefreiheit, werden eventuell in Folgegutachten behandelt.

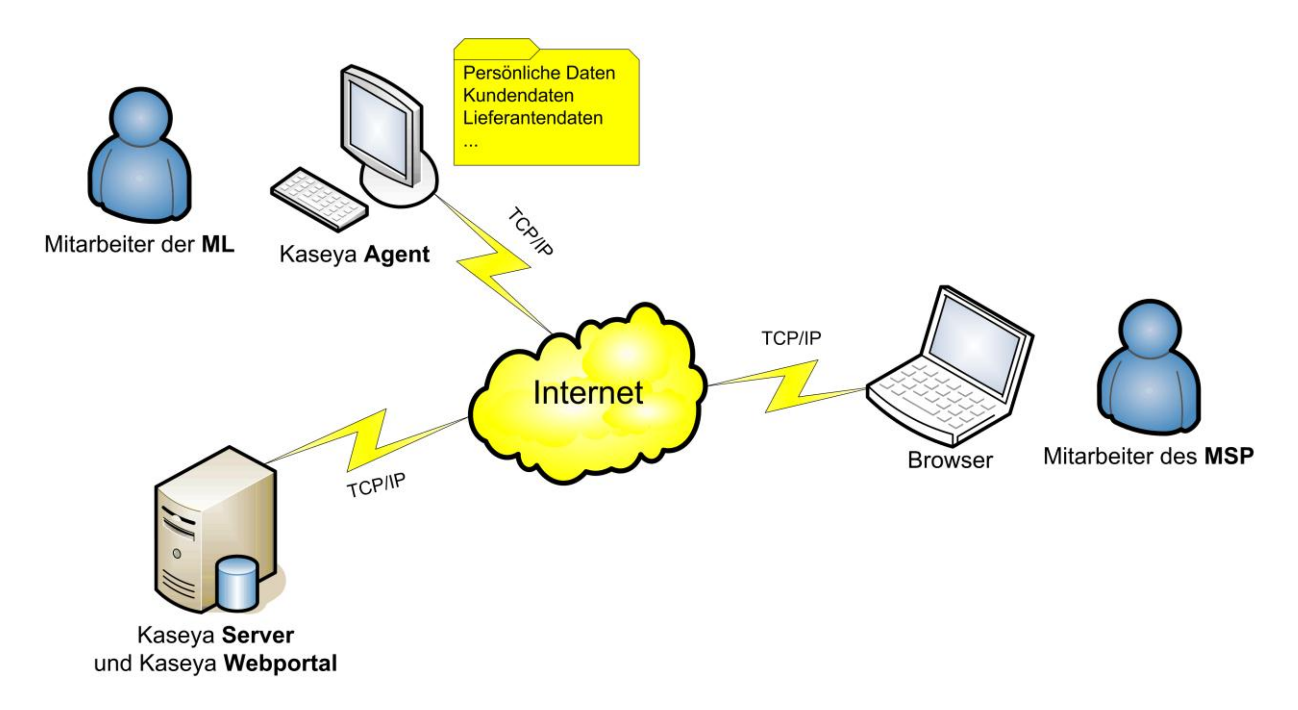


Abbildung 1: Datenschutz Szenarium beim Einsatz des *Kaseya IT Automation Framework*

VORGEHENSWEISE

Auf Basis der Produktdokumentationen wurde zunächst eine Referenzinstallation des *Kaseya IT Automation Framework*[4] entwickelt, darauf aufbauend eine hochschulinterne Testinstallation entworfen und dann die Erhebung sowie Verwendung von personenbezogenen Daten (PBD) im Sinne des Datenschutzrechts in der Referenzinstallation ermittelt und anhand der Testinstallation überprüft. Die Referenzinstallation umfasste dabei den gesamten IT-Verbund inklusive Beteiligten, Rollen, IT-Anwendungen, IT-Systemen, Netzverbindungen, Räumen und Gebäuden.

Hinsichtlich der Erhebung und der Verwendung personenbezogener Daten im Sinne des Datenschutzrechts wurden die nachfolgenden Geschäftsprozesse, die durch das *Kaseya IT Automation Framework* unterstützt werden können, berücksichtigt:

Inventarisierung
Patch Management
Monitoring
Softwareverteilung
Ticketing
Scripting
Reporting
Remote Desktop
Remote Tools
Antivirus / Antispy
Backup / Disaster Recovery
Desktop Policy / Migration
Service Desk

[4] Der gesamten Untersuchung zugrunde liegt die Version **MSE K2** Enterprise Edition 6.0 (VSA 6.0.0.0; KServer 6.0.6.0; KAgent 6.0.0.3) in Verbindung mit dem deutschen Benutzerhandbuch vom 11.6.2010.



Die anschließende Sicherheitsteilanalyse der Referenzinstallation führte dann zu ersten datenschutzkonformen Administrations-, Installations- und Konfigurationsempfehlungen. Danach wurden die IT-Anwendungen, IT-Systeme, Netzverbindungen, Räume und Gebäude der Referenzinstallation der Version MSE K2 anhand der „8 Gebote“ in der Anlage zu § 9 Satz 1 BDSG begutachtet und es wurden datenschutzrechtlich erforderliche, technische und organisatorische Maßnahmen ermittelt, die dem heutigen Stand der Technik entsprechen. Zusätzlich wurden erforderliche Verhaltensregeln und mögliche Verpflichtungen der Beteiligten (etwa: Meldepflichten und Informationspflichten), die sich durch den Betrieb des IT-Verbunds aus den einschlägigen Datenschutzvorschriften ergeben, benannt. Schließlich wurden für die Beteiligten ggf. notwendige bzw. empfehlenswerte Vereinbarungen ermittelt. Hinsichtlich dieser Vereinbarungen wurden allerdings nur empfohlene Inhalte benannt, da eine rechtliche Beratung naturgemäß nicht Gegenstand dieses Gutachtens sein kann. Hier ist ggf. also noch die Mitwirkung eines Fachanwalts erforderlich.



VORBEMERKUNGEN

DATENSCHUTZ

Datenschutz wird in Deutschland als „Verdatungsschutz“ verstanden: Daten, die sich auf eine natürliche Person und deren Lebensumstände beziehen, dürfen nur in Ausnahmefällen und auch dann nur zweckgebunden erhoben und verwendet werden.

Die Ausnahmefälle werden für die Privatwirtschaft vorrangig im **Bundesdatenschutzgesetz (BDSG)** festgelegt. Weitere Regelungen finden sich im **Telemediengesetz (TMG)** und im **Telekommunikationsgesetz (TKG)**. Da das BDSG den Charakter eines Auffanggesetzes hat (§ 1 (3) BDSG), haben die Bestimmungen des TKG und des TMG oft sogar Vorrang. Dazu ist jedoch erforderlich, dass der privatwirtschaftliche Betrieb entweder ein **Diensteanbieter** im Sinne des TMG oder des TKG ist. Ein Diensteanbieter im Sinne des TMG ist jede natürliche oder juristische Person, die eigene oder fremde Telemedien zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt (§ 3 (1) TMG). Im Sinne des TKG ist ein Diensteanbieter jeder, der ganz oder teilweise geschäftsmäßig Telekommunikationsdienste erbringt oder an der Erbringung solcher Dienste mitwirkt (§ 3 (6) TKG). Das TKG ist also anwendbar, wenn der privatwirtschaftliche Betrieb reine Transportleistungen von Informationen erbringt. Das TMG gilt, wenn der privatwirtschaftliche Betrieb eigene oder fremde Informationen im Intranet oder Internet zur Nutzung bereithält.

PERSONENBEZOGENE DATEN

Das BDSG definiert im § 3 (1) den Begriff personenbezogene Daten (PBD) durch: „**Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)**“.

Häufiger Streitpunkt ist die Bedeutung des Begriffes „bestimmbar“ in der gesetzlichen Definition personenbezogener Daten. Reicht es, dass die natürliche Person potenziell bestimmbar ist, oder muss sie realistisch, ja gar rechtmäßig bestimmbar sein? Für beide Sichten gibt es gute Gründe. In Juristenkreisen scheint eine Mehrheit der Meinung, dass eine Einzelangabe zu einer natürlichen Person nur dann ein personenbezogenes Datum ist, wenn die verantwortliche Stelle über Kenntnisse, Mittel und Möglichkeiten verfügt, einen Personenbezug mit den ihr normalerweise zur Verfügung stehenden Hilfsmitteln und ohne unverhältnismäßigen Aufwand herzustellen.

DATENSCHUTZ VERSUS DATENSICHERHEIT

Datensicherheit schafft technische und organisatorische Voraussetzungen, um das von einer Organisation geplante Ausmaß an Vertraulichkeit, Integrität und Verfügbarkeit bei der Erhebung und Verwendung von beliebigen Daten sicherzustellen.

Datenschutz hingegen legt auf Grundlage des jeweils gültigen Datenschutzrechts fest, unter welchen technischen und organisatorischen Voraussetzungen personenbezogene Daten überhaupt erhoben oder verwendet werden dürfen.

Zahlreiche technische und organisatorische Maßnahmen dienen folglich sowohl dem Datenschutz als auch der Datensicherheit. Dies zeigt etwa das Beispiel „Verschlüsselungstechniken“.

Manchmal ergeben sich jedoch aus Datenschutz und Datensicherheit konkurrierende Anforderungen. Dies kann am Beispiel „Vorratsdatenspeicherung“ verdeutlicht werden. Aus Sicht des Datenschutzes sollten dabei so

wenig personenbezogene Daten wie möglich erhoben und genutzt werden. Tatsächlich werden in der Praxis jedoch personenbezogene Protokolldaten oft unbegrenzt erhoben und längerfristig gespeichert, um Angriffe auf die Datensicherheit auch nachträglich erkennen und analysieren zu können.

SPEZIELLE KATEGORIEN VON PERSONENBEZOGENEN DATEN

Bei der Anwendung und Diskussion des Datenschutzrechts ist es oft sinnvoll, gewisse Kategorien von personenbezogenen Daten getrennt zu betrachten.

Man unterscheidet auf oberster Ebene zunächst **Primärdaten** und **Sekundärdaten**. **Primärdaten** sind (weitgehend) statische personenbezogene Daten, wie z.B. Name, Vorname, Geburtsdatum. **Sekundärdaten** sind (weitgehend) dynamische personenbezogene Daten, also abhängig von den aktuellen Lebensumständen des Betroffenen. Dazu gehören etwa Protokolldaten über Dateneingaben und Datenbankzugriffe, Inventardaten eines verwendeten Rechners und Logdaten über den Zugang zu sensiblen Räumen. Die Grenze zwischen Primärdaten und Sekundärdaten ist allerdings nicht immer scharf.

Bestandsdaten sind alle personenbezogenen Daten, die für ein Vertragsverhältnis erforderlich sind, welches die Nutzung einer IT-Anwendung auf einem IT-System prinzipiell erst ermöglicht. Sie gehören zu den Primärdaten.

Beispiele:

- Name des Nutzers,
- Anschrift,
- Email-Adresse und
- Rufnummer.

Nutzungsdaten sind alle personenbezogenen Daten, die erforderlich sind, um eine IT-Anwendung auf einem IT-System tatsächlich zu nutzen. Auch diese gehören zu den Primärdaten.

Beispiel:

- Daten zur Authentifizierung des Nutzers (Benutzerkennung, Benutzerkennwort).

Verkehrsdaten hingegen sind personenbezogene Daten, die die Transportleistungen während der Nutzung einer IT-Anwendung auf einem IT-System beschreiben. Sie gehören zu den Sekundärdaten.

Beispiele:

- Angaben über Beginn und Ende der jeweiligen Nutzung und
- Anzahl der übertragenen Bytes.

Verhaltensdaten bzw. **Leistungsdaten** sind personenbezogenen Daten, die das Verhalten bzw. die Leistung einer natürlichen Person betreffen.[5] Sie gehören zu den Sekundärdaten.

---

[5] Gemäß § 87 Abs. 1 Nr. 6 BetrVG hat der Betriebsrat ein Mitbestimmungsrecht bei der Einführung und Anwendung technischer Einrichtungen zur Überwachung von Verhalten und Leistung eines Arbeitnehmers. Dies mag für den Betrieb des *Kaseya IT Automation Framework* bedeutsam sein, gehört jedoch nicht zum Themengebiet „Datenschutz“.



Beispiele:

- Angaben über genutzte Programme und
- Anzahl der gedruckten Seiten.

Besondere personenbezogenen Daten sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben (§ 3 (9) BDSG). Sie gehören zu den Primärdaten.

Weitere Kategorien sind **Audiodaten** und **Videodaten**, die eine natürliche Person wiedergeben bzw. darstellen. Diese sind wohl eher den Sekundärdaten zuzurechnen.

Die Unterscheidung von Kategorien ist wichtig, da die einschlägigen Gesetze oft unterschiedliche Regelungen für diese Kategorien bei der Erhebung und Verwendung beinhalten. Für besondere personenbezogene Daten finden sich solche Regelungen im BDSG, für Bestands-, Nutzungs- und Verkehrsdaten im TMG bzw. TKG, und für Audio- und Videodaten im StGB, BDSG und KunstUrhG.

ERHEBUNG UND VERWENDUNG VON PERSONENBEZOGENEN DATEN

Das BDSG und andere datenschutzrechtliche Regelungen betreffen folgende Standardoperationen für personenbezogene Daten:

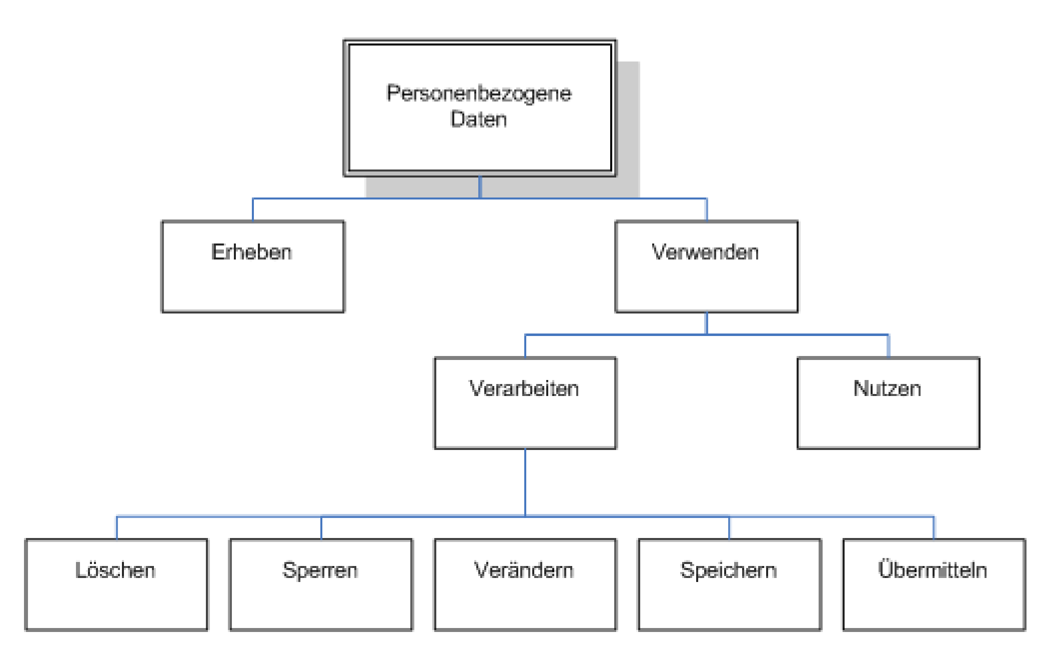


Abbildung 2: Standardoperationen für personenbezogene Daten

Das BDSG definiert im § 3 (3) den Begriff Erheben durch: „**das Beschaffen von Daten über den Betroffenen**“. Das Erheben ist gegeben, wenn es entweder schon durch die Hardware und Software eines IT-Systems geschieht oder manuell zum Zwecke der späteren Speicherung in einer Datei auf einem IT-System erfolgt. Unerheblich ist, ob die Daten mündlich oder schriftlich beschafft werden, ob der Betroffene befragt wird, ob ein Dritter befragt wird oder ob Unterlagen eingesehen werden. Ein Erheben liegt auch vor, wenn die Daten anschließend anonymisiert oder pseudonymisiert verarbeitet werden.

Verarbeiten ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten (§ 3 (4)

BDSG). Verarbeiten ist somit der Oberbegriff für die nachstehend näher erläuterten Einzelhandlungen.

Gemäß § 3 (4) BDSG ist das Löschen von Daten das „**Unkenntlichmachen gespeicherter personenbezogener Daten**“. Von wesentlicher Bedeutung beim Löschen ist der Grundsatz der Datenvermeidung, das heißt der Grundsatz, Daten nur so wenig wie möglich zu speichern. Daraus folgt die Verpflichtung, Daten zu löschen, sobald sie nicht mehr gebraucht werden. Also sind Löschungsfristen ein wichtiges Instrument des Datenschutzrechtes und deswegen auch ausdrücklich in der Aufzählung der Angaben, die der Datenschutzbeauftragte im Verfahrensverzeichnis gemäß § 4e (7) BDSG aufzuführen hat, ausdrücklich aufgeführt. Gemäß § 35 (2) BDSG ist eine Überprüfung von Löschvorschriften spätestens 3 bzw. 4 Jahre nach der Speicherung erforderlich.

Gemäß § 3 (4) BDSG ist das Sperren von personenbezogenen Daten „**das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken**“. Sperrverpflichtungen ergeben sich u.a. aus § 35 (3) und (4) BDSG.

Gemäß § 3 (4) BDSG ist Verändern "**das inhaltliche Umgestalten gespeicherter personenbezogener Daten**“. Verändern ist also jede inhaltliche Umgestaltung gespeicherter Daten mit der Folge, dass sich der Informationsgehalt ändert. Ein Verändern von Daten kann aber auch darin liegen, dass die Daten mit Daten aus anderen Dateien verknüpft werden. In diesem Fall werden die Daten selbst zwar nicht geändert, wohl aber ihr Kontext. Da sie aber nur im Kontext interpretiert werden, werden automatisch Rückschlüsse gezogen. Ändert sich der Kontext, kann sich daher auch die Bedeutung der Daten ändern!

Gemäß § 3 (4) BDSG ist Speichern das „**Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung oder Nutzung**“. Ein datenschutzrelevantes Speichern von Daten liegt also nur vor, wenn die Absicht besteht, die Daten später auch zu verwenden. Kein Speichern ist deswegen das Fertigen und Aufbewahren einer Kopie für Archivierungszwecke.

Übermitteln von Daten ist gemäß § 3 (4) BDSG das „**Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten in der Weise, dass**

- die Daten an den Dritten weitergegeben werden oder

- der Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft".

Das BDSG definiert dazu im § 3 (8): "**Empfänger ist jede Person oder Stelle, die Daten erhält. Dritter ist jede Person oder Stelle außerhalb der verantwortlichen Stelle. Dritte sind nicht der Betroffene sowie Personen und Stellen, die im Inland, in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen**". Da Übermitteln die Bekanntgabe an Dritte meint, ist also eine Weitergabe an den Betroffenen oder an Auftragnehmer im EU/EWR-Bereich keine Übermittlung!

Gemäß § 3 (5) BDSG ist Nutzen „**jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt**“. Die Gefährdung der personenbezogenen Daten ergibt sich ja nicht nur aus ihrer Verarbeitung, sondern insbesondere dann, wenn sie später genutzt werden. Nutzen ist jeder zweckbestimmte Gebrauch der Daten, was eine Handlung mit erkennbarer Wirkung voraussetzt. Jeder Datenschutz wäre ineffektiv, wenn er nicht durch den Auffangtatbestand des „Nutzens“ abgerundet würde. Als Nutzen gilt auch die Veröffentlichung der Daten, soweit diese nicht als Übermittlung angesehen wird.



PRINZIPIEN DES DATENSCHUTZES

Datenschutzpolitisch sollten sich Unternehmen immer an den folgenden, allerdings nicht in jedem Einzelfall erschöpfenden Katalog halten:

1. Es gibt „**unter den Bedingungen der automatisierten Datenverarbeitung kein ‚belangloses' Datum mehr**"[6]: Jedes personenbezogene Datum muss geschützt werden, losgelöst davon, ob es eine sensible Information enthält oder nicht.

2. Die Grundsätze der Datensparsamkeit und der Erforderlichkeit sind zu berücksichtigen. Die Menge personenbezogener Daten muss demnach so gering wie möglich sein. Das zulässige Ausmaß der Verarbeitung und Nutzung hat sich auf den unabdingbar nötigen Umfang zu beschränken.

3. Personenbezogene Daten dürfen nur so lange gespeichert werden, wie sie zur Zweckerreichung erforderlich sind.

4. Die betroffenen Personen sind umfassend zu informieren über den Einsatz und die Funktionsweise des Systems, die Art der verwendeten Daten, den Verarbeitungszweck, ihre Rechte auf Auskunft, Berichtigung und Löschung ihrer Daten usw.

5. Den betroffenen Personen ist die Wahrnehmung ihrer Rechte zu gewährleisten.

6. Den betroffenen Personen sind – wenn irgend möglich - anderweitige Möglichkeiten zur Verfügung zu stellen; es darf keinen faktischen Nutzungszwang für eine automatisierte Datenverarbeitung geben.

DIE 8 GEBOTE DES DATENSCHUTZES

Werden personenbezogene Daten erhoben oder verwendet, sind technische und organisatorische Maßnahmen zu treffen, um die Sicherheit der Datenverarbeitung im Interesse des Schutzes des Persönlichkeitsrechtes zu gewährleisten. Insbesondere wenn personenbezogene Daten automatisiert erhoben oder verwendet werden, sind die Sicherheitsziele der Vertraulichkeit, der Integrität und der Verfügbarkeit zu verwirklichen. Beispielhafte Eignungskriterien für Maßnahmen sind in der Anlage zu §9 Satz 1 BDSG aufgeführt (so genannte „8 Gebote“):

Anlage (zu § 9 Satz 1 BDSG)

Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle),

2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),

3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Da-

[6] Volkszählungsurteil des BVG vom 15.12.1983



ten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),

4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle),

5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogenen Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),

6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),

7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),

8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können (Zweckbindungskontrolle)[7]**.**

Eine Maßnahme nach Satz 2 Nummer 2 bis 4 ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren.

FERNWARTUNG/FERNBETREUUNG

Nach DIN 31051 wird unter **Wartung** „die zur Betriebsbereitschaft notwendige Instandhaltung und Instandsetzung einer Anlage“ verstanden. **Instandhaltung** sind dabei alle vorbeugenden, zur Aufrechterhaltung der Betriebssicherheit der Anlage erforderlichen Leistungen. Hier erfolgt der Zugriff auf die Anlage, um deren Zustand zu überprüfen, indem technische Zustandsdaten abgefragt und analysiert werden (Diagnose). **Instandsetzung** bedeutet die Beseitigung einer Störung an der Anlage durch Reparatur oder Ersatz. Hier erfolgt der Zugriff nur im Falle eines Fehlers.

Die **Wartung von IT-Infrastrukturen** bezieht sich sowohl auf die Hardware als auch auf die Software. Bezüglich der Software wird unter Wartung die Analyse auftretender Fehler und deren Beseitigung sowie das Vorhalten einer optimalen Systemkonfiguration verstanden. Der zunehmende Einsatz von Fremdsoftware führt in der Regel dazu, dass der Benutzer eine Programmpflege und Fehlerbehebungen nicht mehr selbst oder nur beschränkt ausführen kann und in Folge dessen externer Hilfe bedarf. Hiermit verbunden ist für das externe Wartungspersonal oftmals nicht nur eine Zugangsberechtigung zur Software, sondern auch eine Zugriffsberechtigung auf die Daten, um eine effektive Fehleranalyse und erfolgreiche Fehlerbehebung zu ermöglichen.

Die Wartung der Hard- und Software von IT-Infrastrukturen kann sowohl direkt vor Ort als auch durch eine so genannte **Fernwartung** ausgeführt werden.

Unter **Fernwartung** versteht man den (werkzeuggestützten) Fernzugriff von technischem Personal auf IT-Infrastrukturen zu Wartungszwecken. Davon zu unterscheiden ist die **Fernbetreuung**, die die (technische) Unterstützung von Benutzern solcher IT-Infrastrukturen aus der Distanz bezeichnet.

[7] Der Begriff „Zweckbindungskontrolle“ ist eine redaktionelle Einfügung des Autors.

Ein wesentliches Ziel der Fernwartung/Fernbetreuung ist es, die Datenerfassung und die Datenverarbeitung in den Hintergrund treten zu lassen, den Benutzer der IT-Infrastrukturen von Dateneingaben zu entlasten und ihm die gewünschten Funktionen selbsttätig zu bieten oder anzubieten.

In der Privatwirtschaft und der öffentlichen Verwaltung steigt der Bedarf nach Fernwartung und Fernbetreuung stetig. Fernwartung und Fernbetreuung machen es möglich, Zeit einzusparen sowie qualifiziertes Personal und zentrale Ressourcen effizient einzusetzen. Mitarbeitern kann vom Service Desk zeitnah Unterstützung im Problemfall angeboten werden, notwendige Konfigurationsänderungen bzw. Einstellungen an einer Vielzahl von Arbeitsplatzrechnern können auf ein zeitliches Minimum reduziert und neue Softwareversionen auf Servern von Herstellerfirmen aus der Ferne automatisch eingespielt werden, ohne Verzögerungen und Reisekosten.

An jede Fernwartung/Fernbetreuung sind strenge Anforderungen zu stellen, da eine unsachgemäß durchgeführte Maßnahme eine ordnungsgemäße Datenverarbeitung gefährden oder gar eine rechtswidrige Datenverarbeitung darstellen kann, wenn zum Beispiel eine der folgenden Schutzzielverletzungen eintritt:

- Verletzung der Vertraulichkeit durch unbefugte Kenntnisnahme von Daten.
- Verletzung der Integrität durch eine unzulässige Änderung oder Löschung von Daten oder Programmen.
- Verletzung der Verfügbarkeit durch Systemausfall infolge einer Wartungsmaßnahme.

Aus dem **Blickwinkel der IT-Sicherheit**, die ja bekanntlich ein geplantes Ausmaß der Vertraulichkeit, der Integrität und der Verfügbarkeit von IT-Infrastrukturen zum Ziel hat, sollte Fernwartung/Fernbetreuung daher nur mit Einverständnis (aktiver Zustimmung) des betroffenen Mitarbeiters durchgeführt werden. Die Aktivitäten während der Fernwartung/Fernbetreuung sollten immer vom betroffenen Mitarbeiter kontrolliert werden können, etwa durch Beobachtung der Aktivitäten auf dem lokalen Bildschirm. Jede Aktion der Fernwartung/Fernbetreuung sollte protokolliert werden, um eine spätere Revision zu ermöglichen. Die maximale Aufbewahrungsdauer dieser Protokolle sollte festgelegt sein. Der Kreis derer, die überhaupt Fernwartung/Fernbetreuung durchführen dürfen, sollte klar definiert und eng begrenzt sein ebenso wie die Zugangs- und Zugriffsmöglichkeiten im Rahmen der Fernwartung/Fernbetreuung auf das erforderliche Maß zu beschränken sind.

Aus der **Sicht des Datenschutzes** sind bei der Fernwartung/Fernbetreuung weitere Bedingungen einzuhalten.

Dazu sind zwei Arten von Fernwartung zu unterschieden:

- **Fernwartung für eigene Zwecke** ist die interne Anwendung von Fernwartung in großen und/oder verteilten Organisationen, z. B. weitläufige Werksgelände mit mehreren Gebäuden,
- **Fernwartung durch Außenstehende** ist die Fernwartung durch externe Organisationen, z.B. Softwarewartung durch die Herstellerfirma.

Die Fernwartung für eigene Zwecke ist aus datenschutzrechtlicher Sicht wie jedes andere Verfahren innerhalb der verantwortlichen Stelle zu behandeln. Insbesondere ist sie unter den Vorgaben des § 9 BDSG nebst der Anlage zu § 9 Satz 1 BDSG zu betrachten, falls personenbezogene Daten erhoben oder verwendet werden.

Fernwartung durch Außenstehende ist rechtlich als **Datenverarbeitung im Auftrag (DVA)** gemäß § 11 BDSG einzuordnen, da ein Zugriff auf personenbezogene Daten praktisch nie ausgeschlossen werden kann (siehe § 11 (5) BDSG). Insbesondere müssen also Art und Umfang der Wartungsarbeiten differenziert vertraglich geregelt werden. Gleiches gilt für die Verpflichtung des Auftragnehmers, die für den Auftraggeber geltenden datenschutzrechtlichen Bestimmungen einzuhalten, und auch die Untersagung, dass personenbezogene Daten, die im Rahmen der Fernwartung offenbart werden, weitergegeben werden. Die Anforderungen des § 9 BDSG nebst der Anlage zu § 9 Satz 1 BDSG hinsichtlich der technisch-organisatorischen Maßnahmen des Datenschutzes sind aber natürlich auch dieser Art der Fernwartung zugrunde zu legen.



Entsprechend kann man **Fernbetreuung für eigene Zwecke** und **Fernbetreuung durch Außenstehende** unterscheiden. Der wesentliche Unterschied ist aber, dass Fernbetreuung durch Außenstehende regelmäßig eine Funktionsübertragung darstellt, also keine ADV im Sinne des BDSG ist. Zudem ist Fernbetreuung datenschutzrechtlich meist weniger kompliziert, da etwa beim „Service Desk“ oder „Ticketing“ direkter Kontakt zu den Betroffenen besteht und folglich diese effektiv kontrollieren können, ob und ggf. wie personenbezogene Daten erhoben und verwendet werden.



GESCHÄFTSPROZESSE, DIE DIE VERSION MSE K2 UNTERSTÜTZT

Das *Kaseya IT-Automation Framework* dient dem Verfahren der Fernwartung/Fernbetreuung. Dabei ist es für die Geschäftsprozesse unerheblich, ob es im eigenen Hause oder durch Dritte eingesetzt wird.

Folgende Geschäftsprozesse der Fernwartung/Fernbetreuung werden in der Version MSE K2 unterstützt:

Inventarisierung
Patch Management
Monitoring
Softwareverteilung
Ticketing
Scripting
Reporting
Remote Desktop
Remote Tools
Antivirus / Antispy (optional)
Backup / Disaster Recovery (optional)
Desktop Policy / Migration (optional)
Service Desk (optional)

Diese werden – soweit es für das Verständnis dieses Dokuments erforderlich ist - nachfolgend stichwortmäßig hinsichtlich ihrer Hauptmerkmale beschrieben.

INVENTARISIERUNG

Vollständige Automatisierung von Computerinventarisierungen
Akkurate, aktuelle Bestandsaufnahme der Software und Hardware
Überwachung und Aufzeichnung von Änderungen an der Bestandsaufnahme

PATCH-MANAGEMENT

Komplette Automatisierung für Patch-Ermittlung und -Installation
Volle Kontrolle über Installationsort, -methode und -parameter
Zuverlässige und aktuelle Patch-Datenbank
Vollständiges Rollback
Umfassender Überblick über die Systemgeschichte und vollständige Berichte

MONITORING

System-/Netzwerküberwachung
Windows-Ereignisüberwachung
Anpassbare Warnmeldungen
Fernzugriff auf Task Manager
Durchsetzung von Datei-, Anwendungs- und Netzwerkrichtlinien

SOFTWAREVERTEILUNG

Einfache Anwendungsimplementierung
Flexible Zeitplanung
Automatisierte Systemmanagementfunktionen
Ausführliche Fehlerverarbeitung und -berichte

TICKETING

Flexible Konfiguration
Email-Warnmeldungen
Vollständige Speicherung der Problemhistorie

SCRIPTING

Erstellen von Aufgabenbeschreibungen mittels integrierter Script-Sprache. Vorrangig entsprechend einer ‚IF-THEN-ELSE' Struktur.

REPORTING

Die Version MSE K2 bietet standardmäßig u.a. nachfolgende Berichte:

Audit Report
Executive Report
Log Report
Monitoring Report
Patch Report
Service Desk Report
Software Report
Ticketing Report
Backup Report
Security Report
User State Report.

Zusätzlich können eigene Berichte konzipiert und erstellt werden.

Der Zugriff zu Berichten ist abhängig von der Autorisierung. IT-Geräte, die in Berichte einbezogen werden sollen, können durch die Ebenen *Organisation* (Voreinstellung: ALLE), *Rechnergruppe* (Voreinstellung: ALLE) und *Rechner* (Voreinstellung: ALLE) selektiert werden. Dabei sind gewisse Einschränkungen im System integriert. Zusätzlich können Berichte hinsichtlich Verbreitung an Genehmigungen gekoppelt werden.

REMOTE DESKTOP

Konfigurierbare Clients
Sicheres FTP
Sicheres Online-Chatten
Video Streaming für Schulung und Support per Fernzugriff
Verfügbar für Administratoren und Benutzer

REMOTE TOOLS

Richtlinienmanagement
- Energieeinstellungen
- Laufwerkszuordnungen
- Druckerzuordnungen

Desktopstandard-Management
- Desktopstandards
- Benutzereinstellungen
- Sicherung
- Wiederherstellung
- Migration

ANTIVIRUS / ANTISPY (OPTIONAL)

Virenermittlung dank Heuristik und Scannen von NTFS-Datenströmen
Anti-Spyware-Engine zur Beseitigung von Bedrohungen
Schutzschild mit Scan beim Zugriff

BACKUP / DISASTER RECOVERY (OPTIONAL)

Komplett integrierte Lösung, die alle Windows Server und Workstations an verteilten Standorten sichert
Zentrale, webbasierte Verwaltung aller Funktionen einschließlich Ereignisplanung, Backup-Status und Reporting
Konsolidierte und einfach lesbare Benachrichtigungen bei fehlgeschlagenen Zyklen
Universal Restore auf beliebiger Hardware oder virtuellen Rechnern

DESKTOP POLICY / MIGRATION (OPTIONAL)

Geeignet für alle Windows-Umgebungen (95 bis 7)
Richtlinien für den Dateizugriff:
- Für alle Systeme, Gruppen oder bestimmte Computer
- Für eine oder mehrere Dateien
- Vollständige Einschränkung oder definiert für spezifische Anwendungen

Richtlinien für den Netzwerkzugriff:
- Für alle Systeme, Gruppen oder bestimmte Computer
- Integriert mit Software-Bestandsaufnahme
- Gewähren oder Verweigern des Anwendungszugriffs
- Automatisches „Erlernen“ des Anwendungszugriffs
- Option für Benutzerbenachrichtigung
- Nutzungsüberwachung per Computer und Anwendung

Richtlinien für den Anwendungszugriff:
- Für alle, für Gruppen oder für bestimmte Computer
- Auswahl einer oder mehrerer Anwendungen

Sicherheit durch 256-Bit-RC4-Verschlüsselung
HIPAA-konform

SERVICE DESK (OPTIONAL)

Nachverfolgung und Verwaltung von Vorfällen, Service-Anfragen und Änderungsanfragen
Automatische Ticketweiterleitung und Eskalationsverfahren auf der Basis von SLA-Zielen
Nutzung von Kennzahlen für die Bewertung von SLAs
Detaillierte Steuerung des Service-Desk-Zugriffs
Integrierte Knowledge-Base und Datenbank mit bekannten Fehlern
ITIL-Unterstützung
Übergreifende Nutzung von Daten



IT-STRUKTURANALYSE DER VERSION MSE K2

Das Verfahren zur Fernwartung/Fernbetreuung, welches durch das *Kaseya IT-Automation Framework* realisiert werden kann, ist weitgehend automatisiert. Der technische Teil des Verfahrens wird in diesem Kapitel beschrieben. Dabei werden allerdings nur die Komponenten benannt und erläutert, die für die datenschutzrechtliche Begutachtung wichtig sind.

Das Verfahren besteht aus einem Bündel von IT-Anwendungen, die gemeinsam dem Zweck der Fernwartung und Fernbetreuung dienen. Diese IT-Anwendungen benötigen eine technische Infrastruktur, die von Beteiligten mit gewissen Rollen gewartet, betreut, genutzt, geprüft und überwacht wird.

Die hier beschriebene IT-Struktur bezieht sich auf die Fernwartung/Fernbetreuung durch Außenstehende, da dies das komplexere Szenarium darstellt.

Aus Gründen der einfacheren Darstellung und besseren Lesbarkeit wird im Folgenden stets die er-Endung verwendet, wie etwa in Mitarbeiter. Selbstverständlich gibt es auch Mitarbeiterinnen. Alle derartigen Bezeichnungen sind daher geschlechtsneutral zu interpretieren.

BETEILIGTE

HERSTELLER

Der **Hersteller** ist die *GmbH*.

MITARBEITER

Ein Mitarbeiter ist eine natürliche Person, die in einem Unternehmen beschäftigt ist.

MANAGED LOCATION (ML)

Die **Managed Location (ML)** ist ein Unternehmen, das für eine IT-Infrastruktur eine Fernwartung/Fernbetreuung auf Basis des *Kaseya IT Automation Framework* in Auftrag gegeben hat.

MANAGED SERVICE PROVIDER (MSP)

Der **Managed Service Provider (MSP)** ist ein Unternehmen, das mit Hilfe des *Kaseya IT Automation Framework* eine (entfernte) IT-Infrastruktur einer ML administriert.[8]

[8] Prinzipiell kann der MSP natürlich auch rechtlicher und/oder wirtschaftlicher Bestandteil der ML sein.



ROLLEN

ADMINISTRATOR

Generell ist ein **Administrator** ein Mitarbeiter, der für die ordnungsgemäße Funktion eines IT-Gerätes verantwortlich zeichnet. Dafür werden ihm meist weitreichende Rechte bei der Konfiguration und beim Betrieb des IT-Gerätes eingeräumt.

Ein **Systemadministrator** ist nicht nur für einzelne IT-Geräte sondern für eine ganze IT-Struktur als Administrator verantwortlich.

Das *Kaseya IT Automation Framework* benutzt zusätzlich die Begriffe **Master Administrator (Haupt-Benutzer)** und **Standard Administrator (Standardbenutzer)**. Der Master Administrator ist ein Benutzer des *Kaseya IT Automation Framework* mit umfassenden Rechten für alle Funktionen und Daten des *Kaseya IT Automation Framework*. Ein Standard Administrator hingegen ist (je nach Autorisierung durch einen Master oder einen Standard Administrator) in der Funktionalität beschränkt. Diese Beschränkungen beziehen sich

1. auf die Daten, die eingesehen werden können,
2. die Operationen, die für diese Daten gestattet sind (Auswerten, Löschen, …),
3. welche Funktionen im Webportal (siehe unten) zur Verfügung stehen (FTP, …) und
4. wann das Webportal zur Verfügung steht.

Die Autorisierung erfolgt auf Basis eines Rollenmodells mit Umfangsdefinitionen (roles/scopes). Insbesondere kann kein Administrator mehr Rechte für einen von ihm angelegten Administrator autorisieren, als ihm selbst eingeräumt wurden.

Wichtig: Die Einrichtung eines neuen Master Administrator ist <u>jedem</u> möglich, der sich auf dem Webportal-Rechner (siehe MSP-S-1 unten) erfolgreich anmelden kann. Er kann dann über **http://localhost/LocalAuth/setAccount.asp** diese Funktion ausführen.

Eine Besonderheit ist der „**Adminstrator at Remote Location**“. Dies ist ein (Master oder Standard) Administrator, der das Kaseya Server Webportal von einem beliebigen Internetzugang für seine Administrationsaufgaben verwendet.

BENUTZER

Benutzer ist jede natürliche Person (im Hause ML oder MSP), die ein IT-Gerät nutzt.

DATENSCHUTZBEAUFTRAGTER

Der Datenschutzbeauftragte ist eine gemäß BDSG qualifizierte und bestellte natürliche Person, die die Aufgaben u.a. gemäß BDSG für ein Unternehmen wahrnimmt.

ENTWICKLER

Entwickler sind Mitarbeiter, die eine IT-Anwendung (weiter-)entwickeln.

UNTERNEHMENSLEITER

Unternehmensleiter wird hier als Sammelbegriff für die rechtlich in Verantwortung stehende Person eines Unternehmens verwendet. Im Falle einer GmbH ist dies also der Geschäftsführer; bei einer AG etwa der Vorstandsvorsitzende.

NETZPLAN

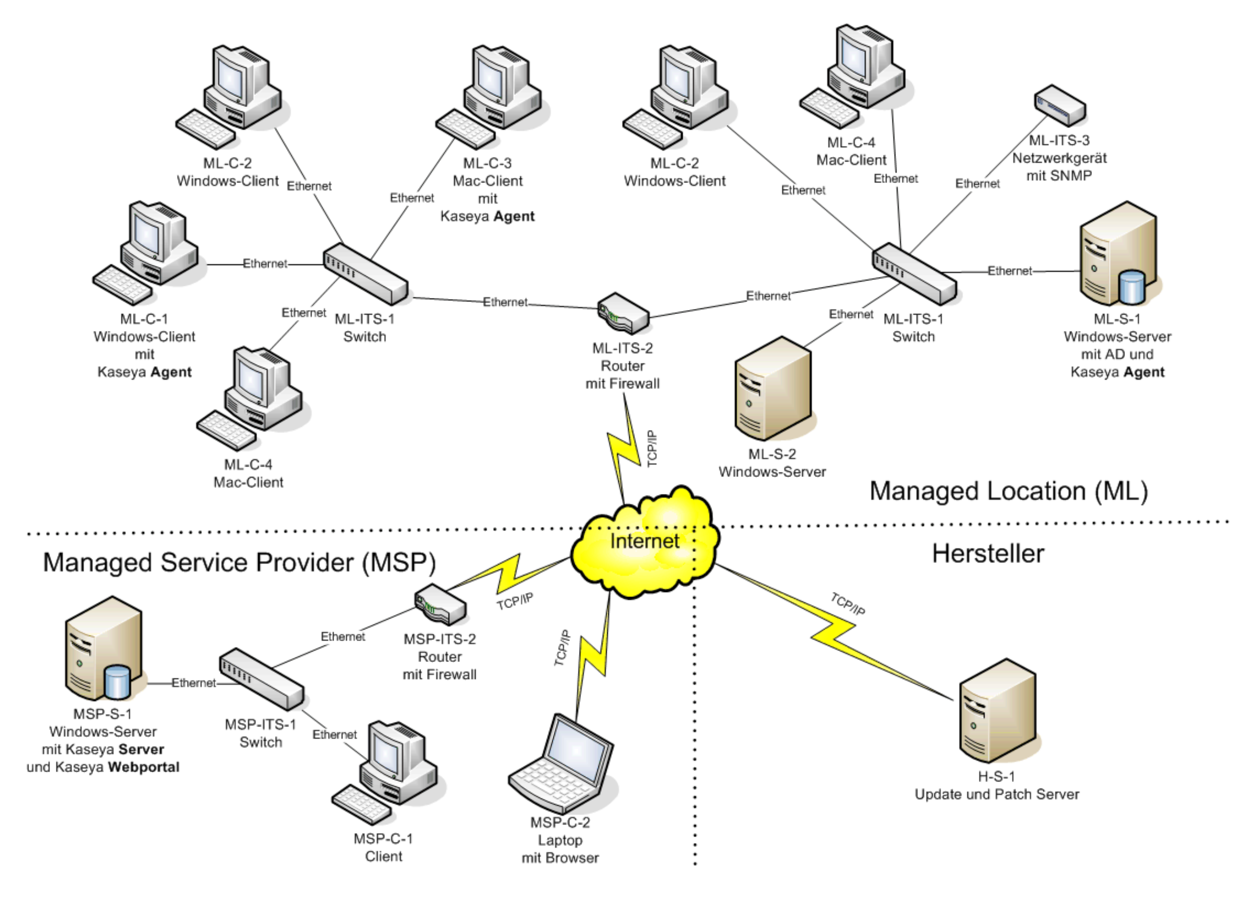


Abbildung 3: Netzplan der Referenzinstallation

IT-ANWENDUNGEN

Nachfolgend erfolgt eine kurze Beschreibung wichtiger Softwarebestandteile der Version MSE K2. Es wird dabei keine Vollständigkeit angestrebt. Vielmehr werden nur die aus Sicht des Datenschutzes wesentlichen Softwarebestandteile behandelt.

KASEYA AGENT

Die Fernwartung eines Rechners innerhalb des *Kaseya IT Automation Framework* basiert auf der Installation einer Software, die als **Kaseya Agent** bezeichnet wird.

Der Kaseya Agent wird automatisch oder manuell auf den fernzuwartenden Geräten der ML als Systemdienst



installiert. Standardmäßig werden dabei folgende Optionen festgelegt:

1. Agentensymbol in der Systemablage anzeigen
2. Benutzer gestatten, den Fernzugriff zu deaktivieren
3. Konteninformationen und IP-Adresse für die Kommunikation mit dem Kaseya Server festlegen
4. Agent kann Kommunikation mit dem Kaseya Server anstoßen
5. Benutzer gestatten, das Agentenprogramm zu beenden.

Alle diese Optionen können jedoch vor und nach der Installation im Kaseya Webportal geändert werden. So ist es im Extremfall möglich, dass der Benutzer des Rechners keinen Einfluss auf den Agenten hat und nur umständlich herausfinden kann (Task Manager), ob der Agent überhaupt aktiv ist.

Bei der manuellen Installation (per Link) muss der Benutzer Administratorrechte auf dem fernzuwartenden Rechner besitzen. Bei der automatischen Installation können die Administratorinformationen des Zielsystems in der Installationsanweisung sicher hinterlegt werden. Diese automatische Installationsanweisung kann dabei – wie bereits angedeutet - so parametrisiert werden, dass die Installation ‚silent' erfolgt, der Benutzer also nicht darüber informiert wird und auch keine Möglichkeit hat, einzugreifen.

Bei der Installation wird für den Kaseya Agent dieses fernzuwartenden Rechners ein **Guid** (Globally Unique Identifier) vergeben, der u.a. auch dazu verwendet wird, Daten und Dateien für die ferngewarteten Rechner auf dem Kaseya Server zu separieren.

Die dem Kaseya Agent zugrunde liegende Konfiguration wird in der Datei **KaseyaD.ini** abgelegt, die regelmäßig durch den Kaseya Server aktualisiert wird. Die Inhalte sind beispielhaft wie folgt:

```
[SERVER COMMUNICATIONS]
User_Name                 winpc.root.ml
Password                  J4bXn7XD
AgentPassword             2f8edd0cf935f9d34421cc31c4d2df2383cbccf29aa42ed31f99e074ebe0d5f7
Server_Name               192.168.0.222
Server_Port               5721
Backup_Server_Name        192.168.0.222
Backup_Server_Port        5721
Revisit_Period            86400
Server_Connection_Timeout 30
Server_Read_Timeout       120
Fast_Check_Period         30
Statistic_Period          3600
Active_Kaseya_Firewall    0
User_Web_Name             http://www.kaseya.com
Firewall_Log              1
NetStats_Log              1
Config_Log                1
Error_Log                 1
Url_Menu_Item_Name
Menu_Items_Enabled        1111111
Notify_User_Denied_NetApp 0
Network_Protect_Enabled   0
NT_App_Event_Log          111111
NT_Sec_Event_Log          111111
NT_Sys_Event_Log          111111
NT_App_Event_Alert        0000000
NT_Sec_Event_Alert        0000000
NT_Sys_Event_Alert        0000000
Exec_Task_Timeout         7200
```

Agent_Guid 286940290146175
Web_Server_Name http://192.168.0.222
Force_Connection_Enabled 1
Event_Log_Cache_Time 86400
Task_Keep_Alive_Time 60
EvtLog_Overflow_Time -1
EvtLog_Overflow_Count -1
Agent_Temp_Dir c:\kworking
Agent_Title
Contact_Menu_Item_Title
Snmp_Concurrent_Threads 30
ExchSvr_Check_Period 43200
Idle_Threshold_Time 600

[MANAGED FILES]
C:\Program Files\Kaseya\FHXSWF95519332180773\KaseyaFW.ini
C:\Program Files\Kaseya\FHXSWF95519332180773\evLogBlkList.xml
C:\Program Files\Kaseya\FHXSWF95519332180773\evLogBlkListEx.xml
C:\Program Files\Kaseya\FHXSWF95519332180773\KaLang.xml

Der Kaseya Agent kommuniziert regelmäßig (mindestens einmal am Tag) mit dem Kaseya Server, indem er eine TCP-Verbindung über den Port 5721[9] aufbaut. Die Kommunikation folgt dem Request/Response-Ansatz: Der Agent fordert Daten an (Request) und der Server liefert diese Daten (Response). Die Kommunikation erfolgt verschlüsselt (256-Bit RC4).

In entsprechenden Intranets kann ein Kaseya Agent auch weitere Rechner, Geräte und - falls **Active Directory (AD)** vorhanden ist - Benutzer durch so genannte ‚Scans' ermitteln. Er verwendet dazu das sogenannte ‚**LAN-Watch**', um weitere Rechner der ML zu entdecken und ggf. mit einem Kaseya Agent auszustatten. Im Falle des AD bezieht er die Daten von einem primären Domain-Controller und diese Konstellation gestattet beispielsweise auch, Benutzer des Kaseya Webportals an die Anmeldeinformationen des AD zu koppeln. Schließlich erlaubt der Kaseya Agent auch das sogenannte ‚**SNMP Monitoring**': SNMP-fähige Geräte können dann über den Agent in die Endgeräte-Verwaltung über diesen Agenten einbezogen werden. Die entsprechenden Aktivitäten werden für den Agenten vom Kaseya Server aus gesteuert.

Allen Agenten werden nach Bedarf per Prozedur Aufgaben (tasks) zugewiesen, die diese – ggf. nach erneuter Kommunikation mit dem Kaseya Server - ausführen. Dazu gehören ***System Agent Procedures***, ***My Procedures*** und ***Public Agent Procedures***. Der Kaseya Server bietet dazu eine Menge von vorgefertigten Prozeduren, die bei Bedarf verwendet werden können. Die folgenden Beispiele zeigen die Vielfalt und – über die Bezeichnung – auch die Funktionen, die sie unterstützen.

System Agent Procedures
Baseline Audit
Disable Windows Automatic Update
Latest Audit
Reset Windows Automatic Update
System Info
Sample Agent Procedures
Agent Control\Force Check-in
Agent Control\Reboot

[9] Die Nummer des Ports ist konfigurierbar. In diesem Dokument wird aber durchgehend die Standardeinstellung verwendet.

Agent Control\Reboot-Ask-No
Agent Control\Reboot-Ask-No-2
Agent Control\Reboot-Ask-Yes
Agent Control\Reboot-Ask-Yes-2
Agent Control\Reboot-Nag
Agent Control\Reboot-Nag-2
Agent Control\Reboot-No-User
Agent Control\Reboot-Warn
Agent Control\Remove K Menu
Agent Control\Remove Startup Task
Agent Control\Reset Audit Cache
Agent Control\Restore App Path RegValue
Agent Control\Startup Task
Config Changes\Disable RegEdit
Config Changes\Execute SNMPWalk
Config Changes\Password Length
Config Changes\Run Windows Script
Managed Services\1 - Computer Cleanup
Managed Services\2 - Server Maintenance
Managed Services\Anti Virus\Check All Virus Defs
Managed Services\Anti Virus\McAfee\Check McAfee Defs
Managed Services\Anti Virus\Stinger\Stinger Step 1
Managed Services\Anti Virus\Stinger\Stinger Step 2
Managed Services\Anti Virus\Stinger\Stinger Step 3
Managed Services\Anti Virus\Symantec\Check Symantec Virus Defs
Managed Services\Anti Virus\Symantec\Install Symantec Antivirus
Managed Services\Anti Virus\Symantec\SAV Network Scan Check
Managed Services\Anti Virus\Symantec\SAV Network Scan step 1
Managed Services\Anti Virus\Symantec\SAV Network Scan step 2
Managed Services\Anti Virus\Trend\Check OfficeScan Defs
Managed Services\Disk Mgmt\Clean\WDC Step 1
Managed Services\Disk Mgmt\Clean\WDC Step 2
Managed Services\Disk Mgmt\Clean\Windows Disk Cleanup (wdc)
Managed Services\Disk Mgmt\Defragmentation\Analyze Defrag Step 1
Managed Services\Disk Mgmt\Defragmentation\Analyze Defrag Step 2
Managed Services\Disk Mgmt\Defragmentation\Auto Defrag 2K
Managed Services\Disk Mgmt\Defragmentation\Dirms Defragger
Managed Services\Network Tests\Ping IP Address 1
Managed Services\Network Tests\Ping IP Address 2
Managed Services\Network Tests\Port Monitor 1
Managed Services\Network Tests\Port Monitor 2
Managed Services\Policy Mgmt\Policy Update 2K
Managed Services\Policy Mgmt\Policy Update XP
Managed Services\Server Mgmt\Set Time Server
Managed Services\Server Mgmt\Backups\Start Services - After Backup
Managed Services\Server Mgmt\Backups\Stop Services - Before Backup
Managed Services\Server Mgmt\Exchange\Exchange Failed Email
Managed Services\Server Mgmt\Exchange\Exchange Mailbox Size
Managed Services\Server Mgmt\Exchange\Verify Exchange database size
Managed Services\Server Mgmt\Terminal Services\TS Port Setting
Managed Services\Spyware\Ad-Aware\Adaware Scan Step 1
Managed Services\Spyware\Ad-Aware\Adaware Scan Step 2
Managed Services\Spyware\Ad-Aware\Adaware Scan Step 3
Managed Services\Spyware\MSAS\Install MSAS
Managed Services\Spyware\MSAS\Uninstall MSAS
Managed Services\Spyware\Spybot\Run Spybot Step 1

Managed Services\Spyware\Spybot\Run Spybot Step 2
Managed Services\System Mgmt\Add Trusted Sites
Managed Services\System Mgmt\Delete Temp Files
Managed Services\System Mgmt\Flush DNS
Managed Services\System Mgmt\Install wGet
Managed Services\System Mgmt\Remote Wake Up
Managed Services\System Mgmt\Renew IP
Managed Services\System Mgmt\Set Agent Naming
Managed Services\System Mgmt\Shutdown
Managed Services\Workstation Management\Default IE Page
Managed Services\Workstation Management\Lock Workstation
Managed Services\Workstation Management\Send Message if Logged On .

Zudem können Agenten so konfiguriert werden, dass sie **SNMP Traps** oder **Alerts** automatisch (per Email) an den Administrator berichten. Zu den wählbaren Alerts gehören z.B. „Low Disk“, „HW Changes“ und „App Changes“.

Durch Klicken auf das Agentensymbol in der Systemablage kann ein Benutzer des ferngewarteten Rechners zudem eine eingeschränkte Version von Kaseya Live Connect (siehe unten) aktivieren, falls er entsprechend autorisiert wurde. Darin stehen ihm – je nach Konfiguration – z.B. Einsichten in die über den ferngewarteten Rechner gespeicherten Daten auf dem Kaseya Server zur Verfügung.

KASEYA SERVER

Der **Kaseya Server** (auch **KServer** oder **Kaseya Server VSA** (Virtual System Administrator) genannt) ist vorrangig für die Kommunikation mit dem Agent verantwortlich. Er hält Aufgaben (tasks) für den Agent bereit und liefert diese auf Anforderung an den Agent. Der Agent nutzt dann diese Aufgaben, um Aktionen (etwa: Defragmentieren eines Sekundärspeichers) oder weitere Kommunikationsvorgänge anzustoßen.

Daneben verwendet Kaseya Server proprietäre Software und Open-Source-Software für weitere Funktionen. Dazu gehören u.a.

ANTIVIRUS

Optional können verschiedene Softwarepakete zur Bekämpfung von Viren eingesetzt werden. Kaseya bietet hier Unterstützung für den Einsatz von u.a. Symantec- und McAfee-Produkten.

BACKUP/RESTORE

Optional kann Software für Backup/Restore-Aufgaben eingesetzt werden.

EMAIL

Eine Softwareanwendung, die das Versenden von Emails auf Basis des Protokolls SMTP ermöglicht.



FTP

Eine Softwareanwendung, die den Austausch von (beliebigen) Dateien auf Basis des Protokolls FTP gestattet. Der Kaseya Server verwendet dazu u.a. das Programm slimftp2.exe[10]. Das Programm muss nicht installiert werden und gestattet, Laufwerke entfernter Rechner wie lokale Laufwerke zu verwenden.

KASEYA LIVE CONNECT (KLC)

Kaseya Live Connect (KLC) fasst die wesentlichen Funktionen für die manuelle Kommunikation mit einem ferngewarteten Rechner zusammen, die dann teilweise auf anderen IT-Anwendungen (etwa K-VNC) beruhen.

Mit dem Ziel der minimalen Benutzerunterbrechung stellt KLC die Werkzeuge bereit, mit denen ein Administrator des MSP einen ferngewarteten Rechner direkt für beliebige Aufgaben einsetzen kann, wie zum Beispiel

1. Einen Dateimanager für das Übertragen von Dateien per Drag & Drop zum und vom ferngewarteten Rechner
2. Eine Eingabeaufforderung (Command-Shell)
3. Einen Remote-Registry-Editor
4. Einen Task-Manager für das Erkennen aktiver Prozesse und des Ressourcenverbrauchs
5. Einen Zugang zu Ereignisanzeigen des ferngewarteten Rechners
6. Eine Ticketing-Benutzeroberfläche für die direkte Aktualisierung noch nicht gelöster Vorfälle
7. Einen Chat für die IM-ähnliche Kommunikation mit dem Benutzer des ferngewarteten Rechners
8. Einen Desktop-Zugriff für den interaktiven Fernzugriff auf den ferngewarteten Rechner
9. Ein Discovery-Werkzeug zur Bereinigung der lokalen Netzwerke eines ferngewarteten Rechners und zur Ermittlung aller Netzwerkknoten
10. Einen Video-Chat mit dem Benutzer des ferngewarteten Rechners, sofern der Rechner über eine Kamera verfügt.

Daneben kann auch der Benutzer eines ferngewarteten Rechners – je nach Autorisierung – über KLC, das er z.B. durch Klicken des Kaseya Agent Icons in der Systemablage startet, eine Verbindung zum Kaseya Server aufbauen und u.a. sein Profil bearbeiten und die zu ihm und dem von ihm benutzten Rechner gespeicherten Daten einsehen.

KASEYA VIDEO PHONE (KVP)

Proprietäre Software für die Videotelefonie.

K-VNC UND WINVNC

Virtual Network Computing, kurz **VNC**, ist ein Softwarepaket, das den Bildschirminhalt eines entfernten Rechners (Server) auf einem lokalen Rechner (Client) – typisch mittels eines „Viewers“ - anzeigt und Tastatur- und Mausbewegungen des Client an den Server zur weiteren Verarbeitung sendet. VNC implementiert das **Remote Framebuffer Protocol** (**RFP**) und ist damit plattformunabhängig einsetzbar.

Da das RFP standardmäßig keine Verschlüsselung enthält, werden generell alle Daten zwischen Client und Server unverschlüsselt über das Netzwerk versendet. Bei der Übertragung sensibler Daten (z. B. Kennworte) besteht daher - wie bei jedem anderen Netzwerkprotokoll - die Gefahr der Ausspähung der Daten.

[10] Dieses Programm wird von vielen Virenscannern als „bedenklich“ eingestuft.

Mit VNC ist es möglich, dass ein Administrator aus dem Hause MSP die Kontrolle über den Rechner eines Mitarbeiters der ML übernimmt, um beispielsweise Software zu installieren oder Fehler zu beheben. Allerdings kann VNC auch als Spionagesoftware missbraucht werden. Viele Implementierungen ermöglichen einen für den Benutzer des überwachten Computers unauffälligen Einsatz.

WinVNC ist ein Produkt der RealVNC Ltd. und implementiert VNC. Zusätzlich zu den Grundfunktionen gemäß RFP bietet WinVNC Authentifizierungen, Verschlüsselungen und eine Text-Chat-Funktion. Die Verschlüsselung erfolgt nach dem Standard AES-128, also AES mit einem 128-Bit-Schlüssel. Mit einem weißen Icon wird – bei entsprechender Konfiguration – auf dem ferngewarteten Rechner angezeigt, dass der Server läuft. Dieses Icon verfärbt sich schwarz, sobald sich ein Viewer mit dem Server verbindet, so dass der Benutzer des ferngewarteten Rechners, auf dem der Server läuft, eine Verbindung bemerkt. Der Server wird im ferngewarteten Rechner standardmäßig mit folgenden Optionen installiert:

1. Accept connections on port 5900
2. Authentication: VNC password
3. Encryption: Prefer on
4. Share files with VNC-Viewers
5. Enable chat
6. Show icon in System Tray
7. Allow VNC-Viewers to connect to VNC-Server
8. Do not prompt VNC-Server user to approve connection
9. Start VNC-Server automatically with Windows

Die aktuelle Version des Servers ist VNC Enterprise Edition E4.5.1. Bei der tatsächlichen Nutzung läuft der VNC-Server im ‚User Mode‘ und wird dann standardmäßig mit den folgenden Optionen genutzt:

1. Accept connections on port 5900
2. Authentication: Windows password
3. Encryption: Always on
4. Share files with VNC-Viewers
5. Enable chat
6. Prompt VNC-Server user to approve connection

K-VNC ist eine proprietäre Version mit ähnlicher Nutzung und vergleichbarem Funktionsumfang. Die aktuelle Version ist K-VNC 4.x.

PCANYWHERE

pcAnywhere ist ein Softwarepaket der Firma Symantec, das ebenfalls dem Fernzugriff auf Rechner dient. Es unterstützt die Betriebssysteme Microsoft Windows, Linux, Mac OS X, und Pocket PC und gestattet die Verschlüsselung der Datenübertragung mit RC4 oder AES.

RADMIN

Remote Administrator (Radmin) ist ein Produkt der Famatech International Corp. Es ist eine Fernzugriffssoftware, die u.a. den Mirror Driver (Video Hook Driver) für die Kontrolle des entfernten Rechners einsetzt und – so jedenfalls die Behauptung des Herstellers – ressourcenfreundlicher ist als andere Fernzugriffssoftware.

Radmin besteht aus zwei Teilen:

Der **Radmin Server** muss auf dem entfernten Rechner installiert werden. Die aktuelle Version ist Radmin Server 3.0[11] und nutzt – standardmäßig – den Port 4899.

Der **Radmin Viewer** gestattet dann auf dem Client die Fernsteuerung.

Die Funktionalität ist ähnlich zu WinVNC. Zusätzlich sind u.a. ein Audio-Chat und eine Unterstützung für Funktionen der **Intel vPro Plattform** (BIOS-Zugriff, Remote-Boot, …) integriert.

Hinsichtlich Sicherheit sind eine Authentifizierung und eine Verschlüsselung des Datenstroms möglich. Die Authentifizierung kann die Windows Authentifizierung (mit und ohne Kerberos) oder ein integriertes System nutzen. Die Verschlüsselung des Datenstroms erfolgt nach AES-256, also AES mit einem 256-Bit-Schlüssel. Allerdings ist bei der Standardinstallation die Verschlüsselung ausgeschaltet.

SPYWARE

Optional können verschiedene Softwarepakete zur Bekämpfung von unerwünschten Programmen eingesetzt werden. Kaseya bietet hier Unterstützung für den Einsatz von u.a. Adaware, MSAS und Spybot.

TERMINAL SERVER

Terminal Server ist eine proprietäre Software für eine „Terminal Emulation“. Insbesondere kann konfiguriert werden, Laufwerke oder Drucker gemeinsam zu nutzen. Damit werden die Laufwerke des Rechners, den der Administrator verwendet, auf dem ferngewarteten Rechner „lokal“.

KASEYA WEBPORTAL[12]

Das **Kaseya Webportal** (manchmal auch **Kaseya Server Web UI** genannt) ist das Portal des *Kaseya IT Automation Framework* und gehört zu der Klasse der Web-2.0-Anwendungen, die u.a. auf Javascript basieren. Die Authentifizierung erfolgt mittels Benutzerkennung und Benutzerkennwort nach dem Challenge-Response-Verfahren (CHAP). Die Kennworte der Benutzer sind gehasht (SHA-1) in der Datenbank gespeichert. Eine ausreichende Kennwortkomplexität (etwa: Mindestlänge, Zeichensätze) wird standardmäßig nicht erzwungen, kann aber eingestellt werden (**System-Serververwaltung-Anmelderegeln**). Bei mehrmaliger Falscheingabe (Standard: 5 x) wird das Benutzerkonto gesperrt.

Befugte Benutzer des Webportals sind Administratoren aus dem Hause MSP aber auch Mitarbeiter aus dem Hause ML, für die ein Portalzugriff (**User Access Account**) eingerichtet wurde.

Jedem befugten Benutzer des Webportals ist stets sowohl eine **Rolle (role)** als auch ein **Umfang (scope)** zugeordnet. Die Rolle bestimmt, welche Funktionen dem Benutzer wann zur Verfügung stehen, und der Umfang bestimmt, auf welche ferngewarteten Rechner diese Funktionen ausgeübt werden dürfen.

Das verwendete Standard-Protokoll für den Portalzugriff ist **http**. Optional kann das Protokoll **https** verwendet werden (also der Einsatz von SSL) und - durch Änderung der Konfiguration (**System-Serververwaltung-Konfigurieren**) - sogar erzwungen werden („Automatisch zu https auf der Anmeldeseite umleiten“).

[11] Antivirussoftware markiert diese Software typisch als „gefährlich“.

[12] Als Ergänzung zum Webportal können **Web Services** auf Basis der Web Services Description Language (WSDL) verwendet werden. Web Services sind aber nicht Gegenstand dieser Untersuchung.

Die Menüstruktur im Webportal ist wie folgt:

Agent
Agent Procedures
Audit
Info Center
Live Connect
Monitor
Patch Management
Remote Control
System
Ticketing

bzw.

Agent
Agent-Verfahren
Fernsteuerung
Info Center
Inventarisierung
Patch-Verwaltung
System
Ticketing
Überwachung

Im Webportal erhält man Zugriff auf einen speziellen ferngewarteten Rechner vorteilhaft über **Inventarisierung – Einzelne Dateien anzeigen - Rechnerübersicht**. Hier kann man über Reiter sowohl Einsicht in alle gesammelten Daten nehmen als auch zahlreiche Aktionen anstoßen (wie Fernzugriff, Chat, Verfahren ausführen, …).

Das Webportal bietet optional u.a. auch Zugriff auf einen Satz von Datenbankansichten, die einen direkten Zugriff auf die Systemdatenbank ermöglichen (**System-Datenbankzugriff-Datenbankansichten**). Diese mit Kennwort geschützten Ansichten können verwendet werden, um Daten z.B. in ein EXCEL-Arbeitsblatt zur Analyse zu übertragen und Berichte vorzubereiten.

MICROSOFT IIS

Internet Information Services (IIS) ist eine Software der Firma Microsoft für PCs und Server. Über sie können Dokumente und Dateien im Intra- und Internet zugänglich gemacht werden. Als Kommunikationsprotokolle kommen hierbei zum Einsatz: HTTP, HTTPS, FTP, SMTP, POP3, WebDAV und andere. Über IIS können ASP- oder .NET-Applikationen (ASP.NET) ausgeführt werden, sowie – mit den passenden installierbaren ISAPI-Filtern – auch PHP und JSP.

MICROSOFT SQL SERVER

Der Microsoft SQL Server ist ein relationales Datenbankmanagementsystem von Microsoft. Er ist grundlegend für den Einsatz des *Kaseya IT-Automation Framework* und mit gewissen Optionen zu installieren. Insbesondere ist neben der Windows-Authentifizierung auch die DB-Authentifizierung erforderlich: Der DB-Administrator (typisch: sa) muss aktiviert sein und Zugriff auf die DB haben.

Die Inhalte der verwendeten Datenbank ***ksubscribers*** sind im Klartext gespeichert, also nicht verschlüsselt oder in anderer Form vor Einsicht geschützt.

Dabei bietet der Microsoft SQL Server (zumindest ab Version 2008) Verschlüsselungsmöglichkeiten, die nicht nur (nahezu) dem Stand der Technik entsprechen, sondern auch relativ leicht in bestehende Anwendungen integriert werden können.

So können Daten, die in SQL Server gespeichert sind, nach einer Methode verschlüsselt werden, die für Anwendungen, von denen eine Verbindung zur Datenbank hergestellt wird, transparent ist. Gerade diese ***transparente Datenverschlüsselung*** ermöglicht es, Datenbankdateien zu verschlüsseln, ohne eine einzige Anwendung ändern zu müssen. Die Verschlüsselung (typisch nach dem Advanced Encryption Standard (AES)) wird nämlich auf Seitenebene durchgeführt, indem die Seiten verschlüsselt werden, bevor sie auf einen Datenträger geschrieben werden, und beim Einlesen in den Speicher wieder entschlüsselt werden. Sicherungsdateien von Datenbanken, für die transparente Datenverschlüsselung aktiviert wurde, werden ebenfalls verschlüsselt.

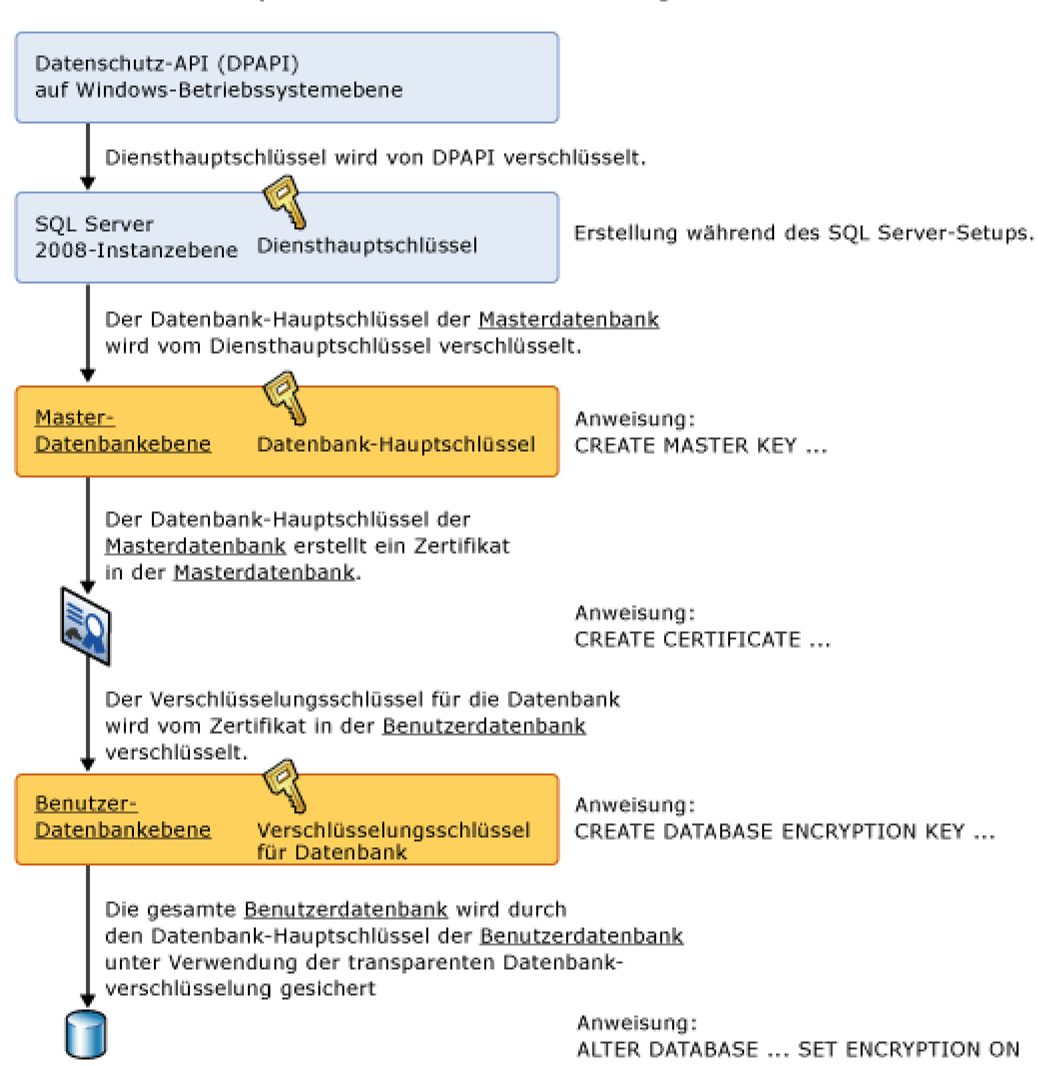


Abbildung 4: Architektur der transparenten Datenverschlüsselung (Quelle: Microsoft)

Anmerkung: Vor einer Aktivierung bzw. Nutzung von Verschlüsselungstechniken ist natürlich abzuschätzen, inwieweit dies Auswirkungen auf die Performanz des Gesamtsystems hat. Hier sind also die IT-Zielsetzungen **Verfügbarkeit** und **Vertraulichkeit** gegeneinander abzuwägen. Aus Sicht des Datenschutzes ist nach Ansicht des Autors regelmäßig der Vertraulichkeit eine höhere Priorität einzuräumen.

IT-SYSTEME

SERVER HERSTELLER

Hier gibt es keine besonderen technischen Anforderungen.

SERVER MSP

Minimale technische Anforderungen sind laut Hersteller:

- Microsoft Windows Server 2003 oder 2008
- Microsoft Internet Information Server (IIS) Version 5.1
- Microsoft Message Queuing (MSMQ)
- Microsoft .NET Framework 3.5
- Microsoft SQL Server 2005 oder 2008
- Microsoft SQL Reporting Services
- Single Processor (2.4 GHz,160 MHz FSB, 1 MB Cache)
- 3 GB RAM
- 40 GB Festplatte
- 100 Mbps Network Interface Card (NIC)

Bei hohen Sicherheitsanforderungen oder hohen Lasten kann der Server auch durch eine zweistufige Architektur implementiert werden. Dabei laufen das Kaseya Webportal und der Kaseya Server auf getrennten Rechnern, die über eine Firewall oder einen Paketfilter miteinander verbunden sind.

Zudem sind redundante Architekturen mit einem primären und einem sekundären Server möglich.

CLIENT MSP

Hier gibt es keine besonderen technischen Anforderungen.

SWITCH MSP

Hier gibt es keine besonderen technischen Anforderungen.

ROUTER MIT FIREWALL MSP

Freigeschaltete Ports:

- Webportal: Port 80 und 443 inbound/outbound
- Email: Port 25 outbound
- Agenten Verbindung: Port 5721 inbound[13]
- Fernzugriffsverbindung: Port 5900 outbound (VNC), Port 4899 outbound (Radmin) [14]

[13] Kann vom Systemadministrator des Kaseya Server geändert werden.

[14] Kann geändert werden.

CLIENT ML

Technische Anforderungen (je nach Optionen):

- 333 MHz CPU oder besser
- 128/256 MB RAM oder mehr
- 30 – 300 MB verfügbarer Platz auf Festplatten oder mehr
- Network Interface Card (NIC)
- Microsoft Windows NT, 2000, XP, 2003, Vista, 2008, 7 oder Apple Mac OS X Version 10.3.9 oder später

SERVER ML

Hier gibt es keine anderen technischen Anforderungen als beim Client ML.

SWITCH ML

Hier gibt es keine besonderen technischen Anforderungen.

ROUTER MIT FIREWALL ML

Freigeschalteter Port:

- Agenten Verbindung: Port 5721 outbound[15]
- Fernzugriffsverbindung: Port 5900 inbound (VNC), Port 4899 inbound (Radmin) [16]

NETZVERBINDUNGEN

ETHERNET

Sowohl beim MSP als auch bei der ML sind 100 Mbps als Minimum gefordert. Je nach Anzahl der ferngewarteten Rechner kann sehr schnell 1+ Gbps erforderlich werden.

INTERNET

Je nach Anzahl der ferngewarteten Rechner gehen die technischen Anforderungen an die Aufschaltung von Modem zu Kabel, DSL , T1 oder besser.

[15] Kann vom Systemadministrator geändert werden.

[16] Kann geändert werden.

HOCHSCHULINTERNE TESTINSTALLATION DER VERSION MSE K2

ITS-2
Drucker
mit SNMP
(192.168.0.200)

ITS-3
Kamera
mit FTP
(192.168.0.150)

C-4
Windows-Client
(192.168.0.4)

Ethernet

ITS-1 Switch
(R1)

C-1 ... C-3
Windows-Client
mit
Kaseya Agent
(192.168.0.1 ... 192.168.0.3)

C-5
Laptop
mit Browser
(192.168.0.111)

S-1
Kaseya Server
mit SQL-DB
(192.168.0.222)

Abbildung 5: Netzplan der Testinstallation

Die hochschulinterne Testinstallation bildet wesentliche Komponenten der IT-Struktur der Version MSE K2 in einem Intranet auf Grundlage des privaten Klasse-C-Netzwerks 192.168.0.0 ab. Die Windows-Clients C1-C4 und der Laptop C-5 haben das Betriebssystem Windows 7. Der Kaseya Server verwendet Windows Server 2008 SP1. Die „Router mit Firewall“ der Referenzinstallation werden durch die Software-Firewall des Betriebssystems nachgebildet.

DATENMODELL DER VERSION MSE K2

Es ist nicht Ziel dieses Kapitels, ein vollständiges Datenmodell der Referenzinstallation der Version MSE K2 darzustellen: Mit Blick auf die Zielsetzung dieses Gutachtens werden nur potenziell datenschutzrelevante Elemente des Datenmodells aufgezeigt.

Für die Angaben in diesem Kapitel zur Datenerfassung, Datenspeicherung und Datenverarbeitung wurde sowohl die Testinstallation im Betrieb beobachtet als auch die zugrunde liegende Datenbank ***ksubscribers*** mit entsprechenden Werkzeugen (u.a. Microsoft SQL Server Management Studio) analysiert.[17] Daneben wurden Dateien im Verzeichnis von MSE K2 (typisch C:\Kaseya) und Angaben des Benutzerhandbuchs ausgewertet.

ERHEBUNG UND VERWENDUNG VON DATEN

Das generelle Szenarium beim Einsatz des *Kaseya IT Automation Framework* ist, dass ein Administrator (aus dem Hause MSP) mittels Software (Agent, Win KNC, …) Daten über einen Rechner und seinen Benutzer (im Hause ML) erhebt und (etwa für Wartungsaufgaben) verwendet.

Ein **Rechner** (**machine**) ist dabei ein Gerät im Hause der ML, das durch das *Kaseya IT-Automation Framework* ferngewartet wird bzw. ferngewartet werden soll. Typisch ist dies ein PC, eine Workstation oder ein Server. Zu den Rechnern gehören jedoch auch z.B. Drucker, die in einem Netzwerk der ML durch PCs genutzt werden. Daher wäre der Begriff IT-Gerät statt Rechner passender. In der Datenbank wird ein solches IT-Gerät durch das Feld **machName** (**Rechner-ID**) identifiziert. Eine typische Wahl für die Rechner-ID ist der konfigurierte Computername des Rechners.

Rechner müssen einer **Gruppe (group)** zugeordnet werden, die auch **Rechnergruppe** genannt werden. Auf Basis dieser Zuordnung können dann der Zugriff auf die Rechner und der Zugriff auf Daten dieser Rechner geregelt werden. Damit wird die Grundlage für einen mandantenfähigen Betrieb des *Kaseya IT Automation Framework* gelegt. In der Datenbank wird eine Gruppe durch das Feld **groupName** (**Gruppen-ID**) identifiziert. Mit K2 wurde für die Gruppen noch **Organisation (org)** als Strukturierungsmerkmal eingeführt. Daher ist die Gruppenkennzeichnung ab Version K2 vom Typ **group.org**[18]. Die Organisation kann dabei selbst noch in Abteilungen oder Unterorganisationen strukturiert werden.

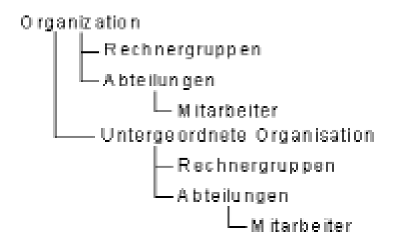


Abbildung 6: Strukturierungsmöglichkeiten in der Version MSE K2 (Quelle: Kaseya)

[17] Schließlich mögen ja Daten erfasst und gespeichert werden, die (noch) nicht standardmäßig angezeigt oder ausgewertet werden.

[18] Gelegentlich wird in den Bildschirmanzeigen die Reihenfolge auch vertauscht und die Darstellung **org.group** verwendet.

Die Bezeichnung der IT-Geräte innerhalb des *Kaseya IT Automation Framework* spiegelt diese Struktur wieder: **winpc.root.ml** ist der Rechner **winpc** in der Gruppe **root** der Organisation **ml.** In der Referenzinstallation kann **winpc** dabei etwa durch ML-C-1 oder ML-C-2 ersetzt werden. Die eindeutige Identifikation eines Rechners innerhalb des *Kaseya IT Automation Framework* erfolgt durch **machName.groupName** (**Rechner-ID.Gruppen-ID**).

Ein **Benutzer (User)** oder **Kontakt** (**Contact**)[19] ist ein Mitarbeiter der ML, der einen Rechner (im oben genannten Sinne) bei seiner Tätigkeit einsetzt. Im Handbuch (siehe z.B. Seite 91) heißt es dazu erklärend: „Person, die den ferngewarteten Rechner benutzt". Demnach wird im *Kaseya IT Automation Framework* regelmäßig davon ausgegangen, dass die Nutzung des Rechners durch den Benutzer weitgehend exklusiv erfolgt. Je nachdem, ob die ML eine private Nutzung des Rechners zulässt, kann folglich nicht ausgeschlossen werden, dass private Daten dieses Benutzers auf dem Rechner vorhanden sind. Zu den privaten Daten gehören häufig Text- und Adressdaten. Aber es können auch Daten zu „persönlichen" Programmen oder zu tragbaren Speichermedien sein. Falls ein generelles Verbot der privaten Internetnutzung nicht besteht, kommen etwa Daten zu Emails und zum Surfverhalten hinzu.

MANUELLE ERHEBUNGEN

Aus Sicht des Datenschutzes von besonderem Interesse ist hier die manuelle Erhebung von Daten, die die Struktur „Organisation-Abteilung-Mitarbeiter" der ML im *Kaseya IT Automation Framework* wiedergeben. Dazu gibt es folgende Datenstrukturen:

Organisation

- Org.-ID – Die eindeutige Kennung der Organisation
- Org.-Name – Der Anzeigename für die Organisation
- Org.-Type – Der Typ der Organisation
- Standardabteilungsname – Die Standardabteilung für die Organisation
- Standardrechnergruppenname – Die Standardrechnergruppe für die Organisation
- Org.-Website – Die Website der Organisation
- Anzahl der Mitarbeiter – Die Anzahl der Mitarbeiter in der Organisation
- Jahresumsatz – Der Jahresumsatz der Organisation
- Bevorzugte Kontaktmethode – Die bevorzugte Kontaktmethode der Organisation: Telefon, E-Mail, Post, Fax
- Übergeordnete Organisation – Die übergeordnete Organisation dieser Organisation
- Die Adresse der Organisation:
  - Land
  - Straße
  - Stadt
  - US-Staat
  - Postleitzahl

Abteilungen der Organisation

- Name – Der Name der Abteilung
- Übergeordnete Abteilung – Die übergeordnete Abteilung
- Managername – Der Name des Abteilungsleiters

---

[19] Die Begriffe *Benutzer* (*User)* und *Kontakt* (*Contact)* werden synonym verwendet. Gelegentlich auch der Begriff *Rechnerbenutzer*. Aus Usability-Sicht ist dies ein Mangel.

Rechnergruppen der Abteilungen der Organisation

- Name – Der Name der Rechnergruppe
- Übergeordnete Gruppe – Die übergeordnete Rechnergruppe

Mitarbeiter der Organisation

- Vollständiger Name – Der volle Name einer Person in der Organisation
- Abteilung – Die Abteilung, mit der die Person verknüpft ist
- Supervisor – Die Person, an die dieser Mitarbeiter Bericht erstattet
- Titel – Der Titel der Person in der Organisation
- Funktion – Die Funktion, in der die Person in der Organisation tätig ist
- Telefonnummer – Die direkte Telefonnummer der Person
- Email-Adresse – Die Email-Adresse der Person
- Benutzerkennung – Das mit diesem Mitarbeiter verknüpfte Benutzerkonto im *Kasey IT Automation Framework*

Bei Einsatz eines **Active Directory (AD)** bei der ML können manche dieser Daten auch teil-automatisiert über einen **Domain Controller** bezogen werden.

Durch Funktionen, die einem Administrator im Hause MSP je nach Autorisierung auf einem ferngewarteten Rechner eingeräumt werden, können im Prinzip <u>sämtliche</u> auf den ferngewarteten Rechnern vorhandenen Daten manuell eingesehen und ggf. manuell mittels FTP übertragen werden.

Diese Funktionen (aus Kaseya Live Connect) umfassen u.a.:

Chat
Command Shell
Event Viewer
File Manager
Registry Editor
Task Manager
Video Chat.

Insbesondere kann über die Command Shell und den Registry Editor - auch unbemerkt vom Benutzer - Hardware an- und abgeschaltet werden. So ist etwa die heimliche Aufnahme von Audio- und Videodaten möglich. Über den Task Manager und den Event Viewer kann das Nutzerverhalten beobachtet und dokumentiert werden.

Aus Sicht des Datenschutzes ebenfalls von Interesse ist die manuelle Erhebung zu Mitarbeitern des MSP. Dazu ein Beispiel aus der Datenbank des Kaseya Servers:

Tabelle 1: Beispiel für „partnerUser“ (Auszug)

ref	admin
partitionid	1
tranId	0
status	1
hasUserData	N
username	Administrator
primaryPartnerUserFlag	N
onVacationFlag	NULL
onSickLeaveFlag	NULL

vacationStartDate	NULL
vacationEndDate	NULL
sickLeaveStartDate	NULL
sickLeaveEndDate	NULL
longitude	NULL
latitude	NULL
mobileFlag	N
mobileType	NULL

AUTOMATISIERTE ERHEBUNGEN

Standardmäßig automatisiert erhebt die Version MSE K2 zumindest die folgenden Daten[20] (u.a. basierend auf den Prozeduren „Baseline Audit“ und „System Info“) für jeden ferngewarteten Rechner[21]:

System Info	Hardwaredaten inklusive Seriennummern etc.
Installed Apps	Alle auf Sekundärspeichern vorhandenen ausführbaren Dateien (*.exe)
Add/Remove	Alle installierten Programme und Programmsysteme
SW Licenses	Softwarelizenzen
Name/OS Info	Betriebssystemdaten
IP Info	Netzwerkkonfigurationsdaten (inkl. IP-Adressen)
DNS/DHCP	Netzwerkkonfigurationsdaten
Disk Volumes	Alle Sekundärspeicher der Maschine
PCI and Disk HW	Hardwaredaten zu PCI und Festplatten
CPU/RAM	Hardwaredaten zu CPU und Primärspeicher
Printers	Installierte Drucker

Beispiele für **winpc.root.ml**[22]:

Tabelle 2: Beispiel für „System Info“

machName	winpc
groupName	root.ml
Manufacturer	ASUSTeK Computer Inc.
Product Name	U3S
System Version	1.0
System Serial Number	NF1G7A03130010
Chassis Serial Number	CSN12345678901234567

---

[20] Diese Daten werden oft nicht nur in der Datenbank sondern auch in gewöhnlichen Textdateien in den Sekundärspeichern des Kaseya Server abgelegt (siehe dazu beispielsweise (bei der Standardeinstellung) C:\Kaseya\MailLog oder C:\Kaseya\UserProfiles)

[21] Im Webportal erreicht man die Daten für einen speziellen ferngewarteten Rechner vorteilhaft über **Inventarisierung – Einzelne Dateien anzeigen - Rechnerübersicht**. Hier kann man über Reiter sowohl Einsicht nehmen als auch Aktionen anstoßen (wie Fernzugriff, Chat, Verfahren ausführen, …)

[22] Die nachfolgenden Beispiele wurden aus den Tabellen (tables) und Ansichten (views) der Datenbank *ksubscribers* extrahiert. Sie sollen vor allem mögliche Inhalte und Detaillierungsgrade verdeutlichen. Daher wurden einige Angaben (wie machName, groupName und agentGuid) häufig aus Darstellungsgründen entfernt.

Chassis Asset Tag	ATN12345678901234567
External Bus Speed	200 MHz
Max Memory Size	8 GB
Max Memory Slots	2
Chassis Manufacturer	ASUSTeK Computer Inc.
Chassis Type	Notebook
Chassis Version	1.0
Motherboard Manufacturer	ASUSTeK Computer Inc.
Motherboard Product	U3S
Motherboard Version	1.0
Motherboard Serial Number	BSN12345678901234567
Processor Family	Intel (r) Pentium (r) M processor
Processor Manufacturer	Intel
Processor Version	Intel(R) Core(TM)2 Duo CPU T7500 @ 2.20GHz
CPU Max Speed	2200 MHz
CPU Current Speed	2200 MHz
emailAddr	NULL
agentGuid	NULL

Tabelle 3: Beispiel für „Installed Apps“ (Auszug)

ProductName	Betriebssystem	HP USB Disk Storage Format Tool	Kaseya Server Email Reader
ProductVersion	6.1.7600.16385	1.0.2003.1113	6.0.1.0
ApplicationName	memtest.exe	HPUSBF.EXE	KEmailReader.exe
manufacturer	Microsoft Corporation	Hewlett-Packard Company	Kaseya
ApplicationDesc	Arbeitsspeicherdiagnose	HPUSBF	Kaseya Server Email Reader
LastModifiedDate	07/14/2009 01:20:36	11/13/2003 09:00:00	05/07/2010 12:11:00
ApplicationSize	485440	450560	278528
DirectoryPath	C:\Boot	C:\DriveKey	C:\Kaseya\KServer

Tabelle 4: Beispiel für „Add/Remove“ (Auszug)

applicationName
Asus_U3_ScreenSaver
Avira AntiVir Personal - Free Antivirus
FreeMind
CrypTool 1.4.21
DVDx
Intel(R) Graphics Media Accelerator Driver
ImageJ 1.39u

Zu den so erfassten Programmen werden weitere Informationen gespeichert, u.a. die Anweisung, die für ein ‚Remove‘ erforderlich ist:

Tabelle 5: Beispiel für „UnInstall“ (Auszug)

displayName	uninstallStr
Asus_U3_ScreenSaver	C:\Windows\ASUS U3 ScreenSaver Uninstaller.exe
Avira AntiVir Personal - Free Antivirus	C:\Program Files\Avira\AntiVir Desktop\setup.exe /REMOVE
FreeMind	C:\Program Files\FreeMind\unins000.exe
CrypTool 1.4.21	C:\Program Files\CrypTool\uninstall.exe
DVDx	C:\Program Files\DVDx\unins000.exe
Intel(R) Graphics Media Accelerator Driver	C:\Windows\system32\igxpun.exe -uninstall
ImageJ 1.39u	C:\Program Files\ImageJ\unins000.exe

Tabelle 6: Beispiel für „SW Licences“ (Auszug)

Publisher	ProductName	LicenseCode	LicenseVersion	InstallDate
Microsoft Corporation	Microsoft Office Visual Web Developer 2007	82503-694-0000007-62196	12.0.4518.1066	20100609
Microsoft Corporation	Microsoft Windows SDK for Visual Studio 2008 SP1 Express Tools for Win32	12345-111-1111111-50605	6.1.5295.17011	20081024
Adobe Systems	Adobe Acrobat 9 Pro - English, Francais, Deutsch	118	9.0.0	20100603
Microsoft Corporation	Microsoft Visual Web Developer 2008 Express Edition with SP1 - DEU	91911-152-0000077-60839	9.0.30729	20081024
Microsoft Corporation	Microsoft Visual Basic 2008 Express Edition with SP1 - DEU	91908-152-0000043-60051	9.0.30729	20081024

Tabelle 7: Beispiel für „Name/OS info“, „IP Info“ und „DNS/DHCP“

ComputerName	Windows-PC
IpAddress	192.168.0.1
SubnetMask	255.255.0.0
DefaultGateway	192.168.0.100
DnsServer1	NULL
DnsServer2	NULL
DnsServer3	NULL
DnsServer4	NULL
DhcpEnabled	NULL
DhcpServer	NULL
WinsEnabled	NULL
PrimaryWinsServer	NULL
SecondaryWinsServer	NULL
ConnectionGatewayIp	192.168.0.100
OsType	7
OsInfo	Ultimate Edition Build 7600
MajorVersion	6
MinorVersion	1
MacAddr	
LoginName	Benutzer
timezoneOffset	-120

Tabelle 8: Beispiel für „Disk Volumes“

DriveLetter	TotalSpace	UsedSpace	FreeSpace	DriveType	VolumeName	FormatType
C	91574	55567	36007	Fixed	Windows7OS	NTFS
D	53048	36920	16128	Fixed	DATA	NTFS
E	7633	6604	1029	Removable		FAT32

Tabelle 9: Beispiel für „PCI and Disk HW“

	Vendor	Product
PCI Network	Vendor ID = 32902	Product ID = 16937
PCI Graphics	Vendor ID = 4318	Product ID = 1064
PCI Multimedia	Vendor ID = 32902	Product ID = 10315
PCI Sys Peripheral	Vendor ID = 4480	Product ID = 1426
Hard Disk	N/A	ST9160827AS v3.AAA

Tabelle 10: Beispiel für „CPU/RAM“

CpuDesc	Intel(R) Core(TM)2 Duo CPU T7500 @ 2.20GHz, Model 15 Stepping 11
CpuSpeed	792
CpuCount	2
TotalRam	2559

Tabelle 11: Beispiel für „Printers“

PrinterName	PortName	PrinterModel
Epson	USB001	Epson EPL 6200
Adobe PDF	Documents*.pdf	Adobe PDF Converter

Zusätzlich gibt es zahlreiche weitere Erfassungen, wie die nachfolgenden Tabellen zeigen:

Tabelle 12: Beispiel für „AgentConfiguration“ (gemäß View)

machName	winpc
groupName	root.ml
firstCheckin	2010-07-07
lastCheckin	2010-12-11
currentUser	Benutzer
lastLoginName	Gast
workgroupDomainType	2
workgroupDomainName	WORKGROUP
lastReboot	2010-12-11 11:05:04.000
agentVersion	6000003
contactName	Benutzer
contactEmail	benutzer@ml.de
contactPhone	01234-56789



contactNotes	
enableTickets	0
enableRemoteControl	0
enableChat	0
loginName	Benutzer
credentialName	Benutzer
primaryKServer	192.168.0.222:5721
secondaryKServer	192.168.0.222:5721
quickCheckinSecs	30
agentTempDir	c:\kworking

Tabelle 13: Beispiel für „AgentConfiguration“ (gemäß Table)

agentGuid	704509723037440
password	4qDWckNX
configServerFilePath	C:\Kaseya\UserProfiles\704509723037440\KaseyaD.ini
configHash	8589caf687a05b980908c89d89c870c7e51c3faa
failedLoginAttempts	0
totalLoginFailures	0
disableUntil	NULL
currAgentPassword	8ced5727063dbb378d93d7359cbac61d3e2dbdea8e39b28384f1ad2e19a891eb
nextAgentPassword	a5cee9a3e7516d99df039ec46d012ff68d8b66d609358c1aa0afa0321f1fd635
contactUrl	NULL
userWebServer	http://www.kaseya.com
urlMenuName	
primaryKServer	192.168.0.222
secondaryKServer	192.168.0.222
KServerPort	5721
KServerRevisit	86400
kserverfastrevisit	30
dofullcheckin	0
statPeriod	3600
firewallLog	30
firewallLogPath	
netStatsLog	30
netStatsLogPath	C:\Program Files (x86)\Kaseya\FHXSWF24306382835718\KasStats.log
configLog	30
configLogPath	C:\Program Files (x86)\Kaseya\FHXSWF24306382835718\KasAgent.log
errorLog	30
errorLogPath	C:\Program Files (x86)\Kaseya\FHXSWF24306382835718\KasError.log
maxLogAge	30
clientIP	192.168.0.1
clientType	curl/7.12.1 (i386-pc-win32) libcurl/7.12.1 OpenSSL/0.9.7d
agentType	0
adminContact	admin@msp.de



contactName	Benutzer
contactEmail	benutzer@ml.de
contactPhone	01234-56789
contactNotes	
enableMenuItems	1111111
agentVersion	6000003
agentFlags	19
netProtect	0
firstCheckin	13.09.2010 16:23
creatorName	
creationDate	13.09.2010 16:06
ntApplicationLog	31
ntSystemLog	31
ntSecurityLog	31
agentSettingChange	
secondaryKServerPort	5721
remoteControl	5
noHwAudit	1
acctCreation	2010-09-13 16:06:08.030
forceNet	1
evLogCacheSec	NULL
keepAliveSec	NULL
bwLimitKbytesPerSec	NULL
agentTempDir	c:\kworking
tzOffsetMin	-120
tooltipTitle	NULL
contactMenuItemName	NULL
eventLogAge	NULL
maxSnmpThreads	NULL
rcLogAge	30
ticAssign	0
agentLang	12
showToolTip	1
workgroupDomainType	2
workgroupDomainName	WORKGROUP
disableCheckinRqst	0
suspendAgent	NULL
dnsComputerName	Windows-PC
monitorLogAge	NULL
monitorLogArchive	NULL
snmpLogAge	NULL
snmpLogArchive	NULL
sysLogAge	30
sysLogArchive	0

rcLogArchive	0
scriptLogArchive	0
alarmLogArchive	0
netStatsLogArchive	0
configLogArchive	0
errorLogArchive	0
exchSvrState	NULL
exchMBoxCount	NULL
monitorActionLogAge	30
monitorActionLogArchive	0
postUpdateScriptId	NULL
agentInstGuid	FHXSWF24306382835718
snmpTrapsEnabled	0
snmpTrapsCommunity	NULL

Tabelle 14: Beispiel für „UptimeHistory“

machName	groupName	eventTime	duration	type	loginName
winpc	root.ml	2010-07-07 19:51:38.000	0	4	Benutzer
winpc	root.ml	2010-07-07 19:51:38.000	67	1	Benutzer
winpc	root.ml	2010-07-07 19:52:45.000	612	1	Benutzer
winpc	root.ml	2010-07-07 20:02:57.000	5	3	Benutzer
winpc	root.ml	2010-07-07 20:03:02.000	61	1	Gast
winpc	root.ml	2010-07-07 20:04:03.000	1842	1	Benutzer
winpc	root.ml	2010-07-07 20:34:45.007	962	2	Benutzer
winpc	root.ml	2010-07-07 20:50:47.000	372	3	Gast
winpc	root.ml	2010-07-07 20:56:59.000	133	1	Benutzer

Obige Tabelle zeigt, ab wann (**eventTime**) und für wie lange (**duration** in Sekunden) der Agent auf dem Gerät aktiv war. Das Feld **type** zeigt Zusatzinformationen an (etwa: 1 – Agent ist angemeldet, kann jedoch keine Verbindung zum KServer herstellen; 2 – Agent ist angemeldet und mit KServer verbunden; 3 – Agent hat sich normal abgemeldet; …). **loginName** gibt an, wer jeweils als Benutzer angemeldet war.

Weiterhin erfasst der Kaseya Agent – je nach Konfiguration mehr oder weniger umfangreich - **Log- und Protokolldaten**[23]:

Tabelle 15: Log-Daten

Agenten-Log	7
Konfigurationsänderungen	7
Netzwerkstatistiken	7
Agentenverfahrensprotokoll	0
Fernsteuerungs-Log	31

[23] Die Bezeichnungen in den nachfolgenden Tabellen entstammen dem *Kaseya IT Automation Framework*. Auch hier besteht hinsichtlich Usability ein Handlungsbedarf.



Alarm-Log	7
Kontrollaktion	31
SYS-Log	31

Tabelle 16: Protokolldaten

Ereignisprotokolle	31
Kontrollprotokolle	31
SNMP-Protokolle	31

Die in der zweiten Spalte der obigen Tabellen angegebenen Löschungsfristen sind die Standardvorgaben in Tagen, wobei 0 bedeutet, dass keine automatische Löschung vorgesehen ist. Dabei ist aber zu beachten, dass statt einer Löschung eine Archivierung nach der festgelegten Anzahl von Tagen festgelegt werden kann.

Zur Illustration der Log-Daten folgen zwei Beispiele für den ferngewarteten Rechner **winpc.root.ml**:

Tabelle 17: Beispiel für Agentenverfahrensprotokoll (Auszug)

Procedures	Last Execution	Status	Admin
Immediate Patch Scan	01.09.2010 12:37	Success THEN	Benutzer
Office Detection Tool	01.09.2010 12:37	Success THEN	Benutzer
Check XML Parser	01.09.2010 12:37	Success ELSE	Benutzer
Patch Scan	01.09.2010 12:39	Success THEN	Benutzer
Legacy Patch Scan	01.09.2010 12:39	Success THEN	Benutzer
Jetzt ausführen - Latest Audit	01.09.2010 12:52	Success THEN	Benutzer
Latest Audit	01.09.2010 12:52	Success THEN	Benutzer
Office Detection Tool	01.09.2010 12:52	Success ELSE	*System*
WUA Patch Scan Check	01.09.2010 12:52	Success THEN	*System*
WUA Patch Scan PreReq2	01.09.2010 12:52	Success ELSE	*System*
WUA Patch Scan PreReq1	01.09.2010 12:52	Success ELSE	*System*
WUA Patch Rescan (x86)	01.09.2010 12:54	Success THEN	*System*
WUA Patch Scan 1 (x86)	01.09.2010 12:54	Success THEN	*System*
WUA Patch Scan 2 (x86)	01.09.2010 12:54	Success THEN	*System*
Get Add/Remove Programs List	01.09.2010 12:55	Success THEN	Benutzer
SW License Audit	01.09.2010 12:55	Success THEN	Benutzer

Tabelle 18: Beispiel für Konfigurationsänderungen (Auszug)

Zeit	Ereignis
11.09.2010 08:34	User set the profile to Name=Max Mustermann, Email=mmustermann@ml.de, Phone=01234-98765
11.09.2010 08:32	Admin admin Sprache des Agenten einstellen auf English
10.09.2010 17:02	Admin admin hat Profil eingestellt auf Contact Name=Benutzer, Contact Email=benutzer@ml.de, Contact Phone=01234-56789, Admin Email=admin@msp.de, Disable Show notes as tooltip
10.09.2010 17:02	Admin admin Sprache des Agenten einstellen auf Deutsch
10.09.2010 16:40	Admin admin gesendete Meldung Hallo …

Von besonderer Bedeutung bei den Protokolldaten sind die Ereignisprotokolle. Es gibt zum einen die Systemprotokolle, die alle Ereignisse für N Tage (in der Standardeinstellung: N=60), die unabhängig von ferngewarteten Rechnern sind, protokollieren. Beispielhaft sehen diese etwa so aus:

Tabelle 19: Beispiel für Systemprotokoll (Auszug)

Admin	Zeit	Beschreibung
System	11.09.2010 08:21	Patch database refresh completed.
System	11.09.2010 08:21	Log archive processed completed
System	11.09.2010 08:20	Patch overrides refresh failed.
System	11.09.2010 08:20	Patch prerequisites refresh failed.
admin	10.09.2010 17:09	Customized color scheme set to Blue
admin	10.09.2010 16:01	Disabled access for Portal Access for user role Test
admin	10.09.2010 16:01	Disabled access for Edit Profile for user role Test
admin	10.09.2010 16:01	Disabled access for Working Directory for user role Test
admin	10.09.2010 16:01	Disabled access for Check-in Control for user role Test
admin	10.09.2010 16:01	Disabled access for Agent Menu for user role Test

Daneben stehen die Ereignisprotokolle, die - etwa im Falle eines Windows-Betriebssystems - die auf dem ferngewarteten Rechner protokollierten und unter Systemsteuerung einsehbaren Ereignisse wiedergeben.

Hier sind **Ereignisse (Events)** der Typen Application, Directory Service, DNS Server, Internet Explorer, Security und System auswählbar, die dann - nach Wahl - jeweils für die folgenden Kategorien gemeldet werden: Error (E), Warning (W), Information (I), Success Audit (S), Failure Audit (F), Critical (C), Verbose (V).

Die gemeldeten Ergebnisse sehen beispielhaft so aus:

Tabelle 20: Beispiel eines Event-Eintrags

machName	winpc
groupName	root.ml
logType	796450521
eventType	Application
eventTime	2010-07-11 09:17:41.000
ApplicationName	LiveUpdt.exe
EventCategory	Error
eventId	1000
username	N/A
computerName	Windows-PC
EventMessage	Name der fehlerhaften Anwendung: LiveUpdt.exe, Version: 2.0.0.0, Zeitstempel: 0x46b06e0b Name des fehlerhaften Moduls: KERNELBASE.dll, Version: 6.1.7600.16385, Zeitstempel: 0x4a5bdaae Ausnahmecode: 0xe06d7363 Fehleroffset: 0x00009617 ID des fehlerhaften Prozesses: 0x11d0 Startzeit der fehlerhaften Anwendung: 0x01cb20d980cbe595 Pfad der fehlerhaften Anwendung: C:\Program Files\ASUS\ASUS Live Update\LiveUpdt.exe Pfad des fehlerhaften Moduls: C:\Windows\system32\KERNELBASE.dll Berichtskennung: 27afc994-8ccd-11df-be0d-001bfcef93fa

Das *Kaseya IT Automation Framework* gestattet dem Administrator zudem die Konfiguration von **Alerts (Alarmen)**, die ggf. Meldungen an den Server seitens des Agenten erfordern:

Tabelle 21: Konfigurierbare Alerts (Auszug)

Alert if the file changed from the last time the file was fetched
Alert when a new device appears on a LAN monitored by LAN watch
Alert when Agent credential invalid
Alert when Agent goes online
Alert when Agent has not checked in for x Min (Hr Day)
Alert when Audit detects any hardware changes on selected machines
Alert when distributed file changed on Agent and was updated
Alert when existing application deleted
Alert when file access violation detected
Alert when network access violation detected
Alert when new application installed
Alert when new patch available
Alert when patch install failed
Alert when selected machines have less than % free space on any fixed disk partition.
Alert when User disables remote control
Alert when Windows Auto Update changed

Falls dann ein entsprechender Alarm eintritt, wird automatisch eine Alert-Email an den Administrator erzeugt, die die näheren Umstände beschreibt. Diese Emails werden auch in der Datenbank gespeichert.

Tabelle 22: Beispiele für „Alert-Emails"

from	benutzer@ml.de
to	admin@msp.de
cc	NULL
bcc	NULL
subject	[winpc.root.ml] Application log generated Warning Event 4113
bodyFileName	NULL
bodyContent	Application log generated Warning Event 4113 on winpc.root.ml For more information see http://www.eventid.net/display.asp?eventid=4113&source=Avira AntiVir Log: Application Type: Warning Event: 4113 Agent Time: 2010-07-12 09:50:03Z Event Time: 07:43:00 AM 12-Jul-2010 UTC Source: Avira AntiVir Category: Infektion Username: SYSTEM Computer: Winpc Description: AntiVir erkannte in der Datei C:\Kaseya\WebPages\ManagedFiles\VSAHiddenFiles\slimftp2.exe verdächtigen Code mit der Bezeichnung 'APPL/SlimFTP.A'!
from	benutzer@ml.de
to	admin@msp.de
cc	NULL
bcc	NULL
subject	Application list on winpc.root.ml has changed
bodyFileName	NULL
bodyContent	New applications are: C:\Users\Benutzer\AppData\Local\Temp\~nsu.tmp\Au_.exe Removed applications are: C:\DriveKey\HPUSBF.EXE C:\DriveKey\HPUSBFW.EXE C:\Program Files\InstallShield Installation Information\{0E0DF90C-D0BA-4C89-9262-AD78D1A3DE51}\Setup.exe C:\Program Files\MPEG Recorder\MPEGRecorder.exe C:\Program Files\MPEG Recorder\unins000.exe C:\Program Files\NavGear\Content Manager\contentmanager.exe C:\Program Files\NavGear\Content Manager\uninst.exe

Schließlich können für Personen und Rechner, die in Domänen mit Active Directory residieren und dort ferngewartet werden, u.a. folgende Daten automatisch erfasst werden:

Tabelle 23: Datenfelder der Rechnerinformationen aus einem Active Directory (Auszug)

Name	AD-Computername
CanonicalName	Kanonischer Name
DomainName	Domain-Name
DistinguishedName	Eindeutiger AD-Name
OperatingSystem	Betriebssystem
OperatingSystemVersion	Betriebssystemversion
LastLogon	Zeit des letzten Neustarts des Rechners
LastLogoff	Zeit des letzten Herunterfahrens des Rechners
DNSHostName	DNS-Hostname
WhenCreated	Zeitpunkt, zu dem der Rechner Mitglied von AD wurde
WhenChanged	Zeitpunkt, zu dem die AD-Eigenschaften/Rolle des Rechners aktualisiert wurden

Tabelle 24: Datenfelder der Personeninformationen aus einem Active Directory (Auszug)

logonName	AD-Benutzername
CanonicalName	Kanonischer Name
DomainName	Domain-Name
DistinguishedName	Eindeutiger AD-Name
mail	E-Mail-Adresse des Benutzers
phone	Telefonnummer des Benutzers
givenName	Vorname des Benutzers
surName	Nachname des Benutzers
LastLogon	Zeitpunkt, zu dem sich der Benutzer das letzte Mal anmeldete
LastLogoff	Zeitpunkt, zu dem sich der Benutzer das letzte Mal abmeldete
SAMAccountName	SAM-Account-Name (Konto-Anmeldename vor Win-2K)
Beschreibung	Beschreibung des Benutzerkontos
WhenCreated	Zeitpunkt, zu dem der Benutzer Mitglied von AD wurde
WhenChanged	Zeitpunkt, zu dem die AD-Eigenschaften des Benutzers aktualisiert wurden
PwdLastSet	Zeitpunkt, zu dem das Passwort das letzte Mal festgelegt wurde

Hinsichtlich Netzwerknutzung können u.a. folgende Daten über einen Agenten erfasst werden:

Tabelle 25: Datenfelder der Netzwerkstatistik (Auszug)

EventTime	Zeitstempel-Zeichenfolge
BytesRcvd	Anzahl der während dieser Statistikperiode empfangenen Byte
BytesSent	Anzahl der während dieser Statistikperiode gesendeten Byte
ApplicationName	Name der Anwendung, die das Netzwerk verwendet

Für die bei der Fernbetreuung anfallenden Daten sei – stellvertretend – der Bereich „Ticketing“ etwas näher dargestellt.

Tabelle 26: Datenfelder der „Ticket Summary“ (Auszug)

TicketID	Eindeutige ID-Nummer des Tickets
Machine_GroupID	Eine verkettete Darstellung der Rechner-ID und der damit verknüpften Gruppen-ID.
agentGuid	Ein global eindeutiger Identifikator eines Rechner-ID/Gruppen-ID-Kontos und seines entsprechenden Agenten
machName	Der für den Agenten verwendete Rechnername
groupName	Der für den Agenten verwendete Gruppenname
TicketSummary	Ein kurze Beschreibung des Tickets
Administrator	Der Admin-Name, dem dieses Ticket zugewiesen ist
CreatedBy	Admin-Name (oder Rechner-ID, falls vom Benutzer angegeben) der Person, die das Ticket erstellt hat
CreationDate	Zeitstempel der Ticketerstellung
DueDate	Fälligkeitsdatum des Tickets

LastModifiedDate	Datum, an dem die letzte Anmerkung für dieses Ticket eingegeben wurde
ResolutionDate	Zeitstempel der Schließung des Tickets
UserName	Der Name des Absenders.
UserEmail	Die E-Mail-Adresse des Absenders
UserPhone	Die Telefonnummer des Absenders

Aus Sicht des Datenschutzes schließlich von Interesse sind die automatisierten Erhebungen zu Mitarbeitern des MSP. Dazu zwei Beispiele aus der Datenbank des Kaseya Servers:

Tabelle 27: Beispiel für „administrators“

adminName	admin
adminPassword	cover2615ec01fd0bfee3493893576849dce7883bbe32
adminType	2
failedLoginAttempts	3
totalLoginFailures	0
disableUntil	1980-01-01 00:00:00.000
sessionId	17467186
adminIp	192.168.0.222
creationDate	NULL
lastLogin	15.09.2010 10:56
sessionExpiration	15.09.2010 12:01
chatStart	0
forceNewPassword	NULL
lastPasswordChange	NULL
lastAdminGroupId	2
defaultAdminScope	2
lastAdminScope	2
lastAdminScopeStr	2
currentPartitionId	1
partitionStr	1
firstName	Fritz
lastName	Supermann
securityQuestion	Name der Großmutter
securityAnswer	Superoma
defaultAdminGroupId	2

Tabelle 28: Beispiel für „adminHistory“

adminName	**eventTime**	**tabName**	**functionName**
admin	15.09.2010 10:56	Fernsteuerung	Kontrollrechner
admin	15.09.2010 10:57	System	Persönliche Einstellungen
admin	15.09.2010 10:57	System	Statistiken
admin	15.09.2010 10:57	System	Anwendungsprotokollierung
admin	15.09.2010 10:57	System	Systemprotokoll
admin	15.09.2010 10:58	System	Benutzerhistorie

admin	13.09.2010 16:06	Agent	Agentenstatus
admin	13.09.2010 16:07	Agent	Agentenprotokolle
admin	13.09.2010 16:07	Agent	Protokollhistorie
admin	13.09.2010 16:08	Agent	Agentenprotokolle
admin	13.09.2010 16:08	Agent-Verfahren	Zeitplan/Erstellen
admin	13.09.2010 16:09	Info Center	Posteingang
admin	13.09.2010 16:09	Agent	Agentenstatus
admin	13.09.2010 16:09	Agent	Profil bearbeiten

MANUELLE VERWENDUNGEN

Manuelle Verwendungen können naturgemäß vielfältig sein. Tatsächlich gibt es technisch kaum eine Begrenzung. Lediglich durch eine entsprechende Administration und Konfiguration kann (und muss) hier eine Begrenzung stattfinden.

AUTOMATISIERTE VERWENDUNGEN

Hinsichtlich der automatisierten Verwendung von Daten im *Kaseya IT Automation Framework* ist hier vorwiegend die Berichtserstellung zu nennen. Als Standardberichte sind die folgenden in MSE K2 vorgesehen:

Audit:
- Aggregate Table
- Disk Utilization
- Inventory
- Machine Changes
- Machine Summary
- Network Statistics

Executive:
- Executive Summary

Logs:
- Admin Notes
- Agent Log
- Alarm Log
- Configuration Changes
- Event Logs
- Event Logs Frequency
- Log Monitoring
- Network Statistics Log
- Remote Control
- Agent Procedure Log

Monitoring:
- Logs
- Monitor 95th Percentile
- Monitor Action Log
- Monitor Alarm Summary
- Monitor Configuration
- Monitor Log
- Monitor Set
- Monitor Trending
- Uptime History

Patch:
- Patch Management



Software:
- Software Applications Changed
- Software Applications Installed
- Software Licenses
- Software Licenses Summary
- Software Operating Systems

Ticketing:
- Customizable Ticketing
- Ticketing

Dabei kann meist eine Datenauswahl auf den Ebenen Organisation, Gruppe (Rechnergruppe) und/oder Rechner (teilweise auch mit Wildcards) erfolgen. Zudem kann für Berichte festgelegt werden, ob eine Verbreitung genehmigungspflichtig ist. Auch können Filter eingesetzt werden. Eine Veröffentlichung eines Berichtes bedeutet, dass der entsprechende Bericht in den Posteingängen der Empfänger abgelegt wird.

Der Bericht „Executive Summary" hat beispielsweise folgende Inhalte[24]:

Tabelle 29: Inhalte „Executive Summary"

So lesen Sie diesen Bericht:	
Systemabläufe	Audits Completed - The total number of times machines have been audited for hardware and software changes.
	Customer Specific - The total number of times machines... (based on customer criteria).
	Backups Completed - The total number of times machines have been successfully backed up.
Ticketstatus	This section provides a quick overview on the status of Help Desk Tickets. A good status indication is that there are no overdue tickets and more closed tickets than open tickets.
Verwendeter Plattenspeicherplatz	Displays the percentage of hard drive space used on either all machines or just servers. These relate to network drives or shared folders. A good status indicator is that the space used is less than 60%.
Netzwerk-Leistungsauswertung	This is a weighted average calculation that provides an At a Glance overall all network health score. Individual items are scored 0% (lowest) to 100% (highest). Scores are totaled, averaged and weighted to generate a percentage.
Betriebssysteme	Displays the different Windows operating system platforms installed on machines in the network. A good status indicator is that all mission critical machines or server have Windows 2000 or higher installed.

[24] Dies ist Teil des Berichtes auch bei Nutzung der deutschen Sprache als Voreinstellung. Hinsichtlich Usability ebenfalls ein Mangel.

Patch-Status	Displays the current number of patches needing to be installed on machines in the network. A good status indicator is zero un-scanned machines and a very low number of machines missing patches. Also includes number of patch scans completed and the number of patches installed.
Alarmmitteilungen	Displays the total number of each alarm notification generated. Alarms are not generally bad or good. Alarms are the result of proactive monitoring of key system elements. Alarms provide the basis for behind the scene actions that keep the network healthy and operational.
Überblick über Lizenzen	Displays the total of all Microsoft Server, Workstation and Office licenses.

ERHEBUNG UND VERWENDUNG VON DATEN MIT PERSONENBEZUG

In diesem Abschnitt wird untersucht, ob und wie personenbezogene Daten im Sinne des BDSG in der Referenzinstallation der Version MSE K2 erhoben oder verwendet werden.

Obgleich es keine „belanglosen" personenbezogenen Daten gibt (siehe Seite 17), wird dabei zum besseren Verständnis gelegentlich ein erläuterndes Beispiel aufgeführt.

PRIMÄRDATEN

Personenbezogene Primärdaten werden nur zu Mitarbeitern der ML oder des MSP erhoben und verwendet.

Für die **Mitarbeiter der ML** sind dies potenziell die folgenden Daten (siehe Seite 40 f):

1. Vor- und Nachname der Person
2. Die Abteilung, mit der die Person verknüpft ist
3. Die Person, an die dieser Mitarbeiter Bericht erstattet
4. Der Titel der Person
5. Die Funktion, in der die Person tätig ist
6. Die direkte Telefonnummer der Person
7. Die Email-Adresse der Person
8. Das mit dieser Person verknüpfte Benutzerkonto (Benutzerkennung, Benutzerkennwort) im Kaseya Webportal (falls vorhanden)

Diese Daten können sowohl vom Administrator im Hause MSP als auch vom Mitarbeiter der ML – falls autorisiert - selbst im Webportal gepflegt werden.

Hinzu kommen potenziell über die Verknüpfung zu ferngewarteten Rechnern (siehe Seite 45 f)[25]:

---

[25] Im Handbuch (siehe etwa Seite 91) heißt es dazu im Zusammenhang mit der Agentenkonfiguration: „Geben Sie den Namen, die Email-Adresse und die Telefonnummer der Person ein, die den verwalteten Rechner benutzt."

9. Die eindeutigen Kennungen **Rechner-ID.Gruppen-ID** aller ferngewarteten Rechner, die diese Person benutzt (falls vorhanden)
10. Freitextinformationen zum Mitarbeiter (Kontakt Notizen) für jeden benutzten Rechner.

Falls Mitarbeiter der ML nicht separat sondern nur im Zusammenhang mit ferngewarteten Rechnern erfasst werden, verbleiben aus dieser Liste nur die Punkte 1, 6, 7, 9 und 10.

Die Daten der Punkte 1 – 7 sind bezogen auf das Kaseya Webportal Bestandsdaten. Die Daten der Punkte 8 und 9 sind Nutzungsdaten.

Für die **Mitarbeiter des MSP**, typisch Kandidaten für eine Administratorposition, werden potenziell im *Kaseya IT Automation Framework* u.a. folgende personenbezogenen Primärdaten erhoben und verwendet (siehe Seite 54 f):

1. Das mit dieser Person verknüpfte Benutzerkonto (Benutzerkennung, Benutzerkennwort) im Kaseya Webportal
2. Vor- und Nachname
3. Email-Adresse

Hinzu kommen potenziell über die Verknüpfungen zu den von diesem Mitarbeiter ferngewarteten Rechnern (siehe Seite 46 f):

4. Die eindeutigen Kennungen **Rechner-ID.Gruppen-ID** aller ferngewarteten Rechner, die diese Person administriert (falls vorhanden)

Die Daten der Punkte 2 und 3 sind bezogen auf das Kaseya Webportal Bestandsdaten. Die Daten des Punktes 1 sind Nutzungsdaten.

SEKUNDÄRDATEN

Für einen ferngewarteten Rechner, der ja (regelmäßig) eins-zu-eins an Mitarbeiter der ML gekoppelt ist, werden vielfältige Daten erhoben, die sich dann auch auf den Benutzer beziehen. Gleiches gilt für Daten, die beim Fernzugriff, beim Service Desk und beim Backup/Restore entstehen.

Personenbezug, also **Angaben über persönliche oder sachliche Verhältnisse der Mitarbeiter der ML**, kommt dabei vor allem den folgenden Daten zu (siehe Seite 42 f):

1. Rechner
   a. Administrator Email, Kontakt Name, Kontakt Email, Kontakt Telefon, Kontakt Notizen, Kontakt Benutzerkennung.
2. Tickets:
   a. Administrator, Kontakt Name, Kontakt Email, Kontakt Telefon, Inhalt.
3. Alert-Emails:
   a. Absender, Empfänger, Inhalt.
4. Historie (Rechnernutzung):
   a. Benutzerkennung, Zeitpunkt, Dauer.



5. Hardware Audit:

    a. Alle vorhandenen Sekundärspeicher.

6. Software Audit:

    a. Alle installierten Programme und Programmsysteme.
    b. Alle auf Sekundärspeichern vorhandenen ausführbaren Dateien (*.exe).

7. Monitoring:

    a. Dienste.
    b. Prozesse.
    c. Ereignisse.

8. Sonstiges:

    a. Benutzerbeobachtung.
    b. Dateieinsicht/Dateiübertragung.
    c. Backup-Dateien.

Der Personenbezug bei Punkt 2 kann etwa dadurch entstehen, dass der Benutzer „Schulung erforderlich“ bei der Erstellung eines Tickets angibt. Bei Punkt 3 kann auf einen Virenfund, also ein mögliches Fehlverhalten des Benutzers, verwiesen werden. Bei Punkt 4 wird die Arbeitszeit am Rechner erfasst.

Der mögliche Personenbezug gemäß den Punkten 5a, 6a und 6b kann etwa folgendermaßen entstehen:

> Ein wichtiges Hilfsmittel für Diabetiker ist das Führen eines Tagebuchs. Es enthält - idealerweise- alle relevanten Daten der Diabetes-Therapie wie Datum, Uhrzeit, BZ-Höhe, BE, Insulindosis, Tabletten, besondere Anmerkungen. All diese Daten kann ein Diabetiker aus seinem Messgerät zeitnah in die Software **SiDiary** importieren und vorteilhaft einsetzen.

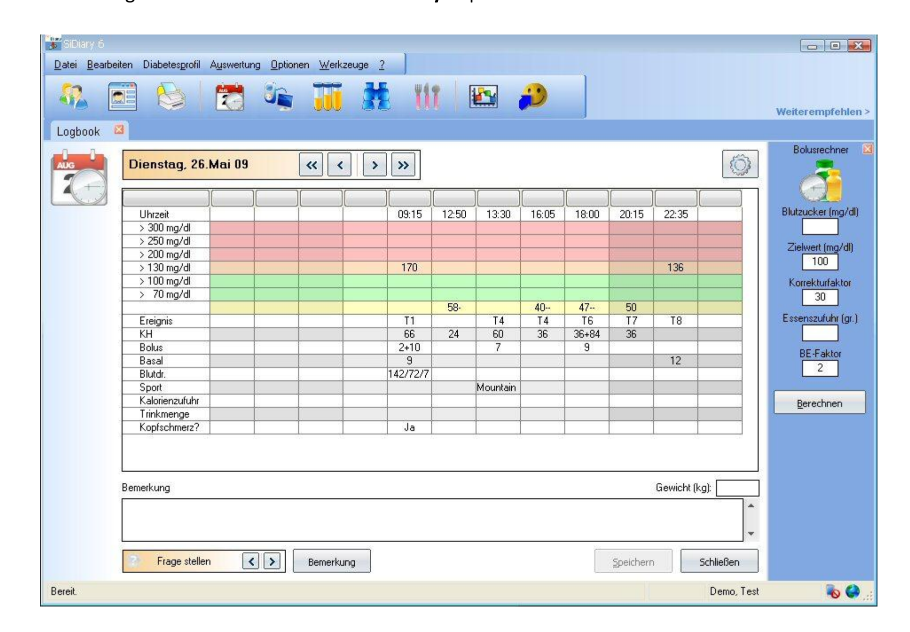


Abbildung 7: Screenshot SiDiary

> Die Existenz der Datei **SiDiary6Setup.exe** etwa auf einem USB-Stick des ferngewarteten Rechners oder die Auflistung von **SiDiary** unter „Installed Apps“ auf einem ferngewarteten Rechner weist die Person, die diesen Rechner nutzt, also mit an Sicherheit grenzender Wahrscheinlichkeit als **Diabetiker** aus.

Bei Punkt 7 kann ein Verhalten bzw. Fehlverhalten des Benutzers erfasst werden. Bei Punkt 8 können ggf. Daten aus persönlichen Verzeichnissen mit personenbezogenen Daten des Benutzers auf einen anderen Rechner übertragen werden (etwa Adressbücher von Email-Programmen oder Kundendaten der ML).

Angaben über persönliche und sachliche Verhältnisse der Mitarbeiter der MSP kommen bei den Sekundärdaten vor allem im Log- und Protokollbereich vor. Hier ist insbesondere zu nennen (siehe Seite 50 f):

1. Historie (Nutzung Webportal):
    a. Benutzerkennung, Zeitpunkt, Funktion.
2. Historie (Konfigurationsänderungen Webportal):
    a. Benutzerkennung, Zeitpunkt, Aktion.

Einen Überblick über die potenzielle Erhebung personenbezogener Daten gibt die Abbildung auf der folgenden Seite. Die in Rot angegebenen Datenbezeichnungen verdeutlichen dabei die Schlüsselfelder, die einen Personenbezug erst erlauben, zumindest wenn – wie allgemein üblich – Benutzerkennungen und Email-Adressen tatsächlich personengebunden vergeben werden[26].

Hinsichtlich der **Verwendung personenbezogener Daten** in der Version MSE K2 sind die Prozesse Speichern, Verändern und Löschen vorgesehen. Eine Sperrung ist technisch nicht möglich. Ein Übermitteln ist äußerst unwahrscheinlich, da dies eine Übertragung an Dritte erfordert, die zwar technisch möglich aber dem Grundgedanken des Einsatzes des *Kaseya IT Automation Framework* entgegensteht. Hiervon ausgenommen ist natürlich eine Übermittlung etwa an Organe der Strafverfolgung. Eine Verwendung außerhalb der Verarbeitung ist die Berichtserstellung, die – wie geschildert – recht breit angelegt ist, und die per Fernzugriff mögliche Dateiübertragung.

[26] Aus Gründen der Revisionssicherheit ist diese personengebundene Vergabe sogar ein Muss im Bereich Fernwartung/Fernbetreuung.

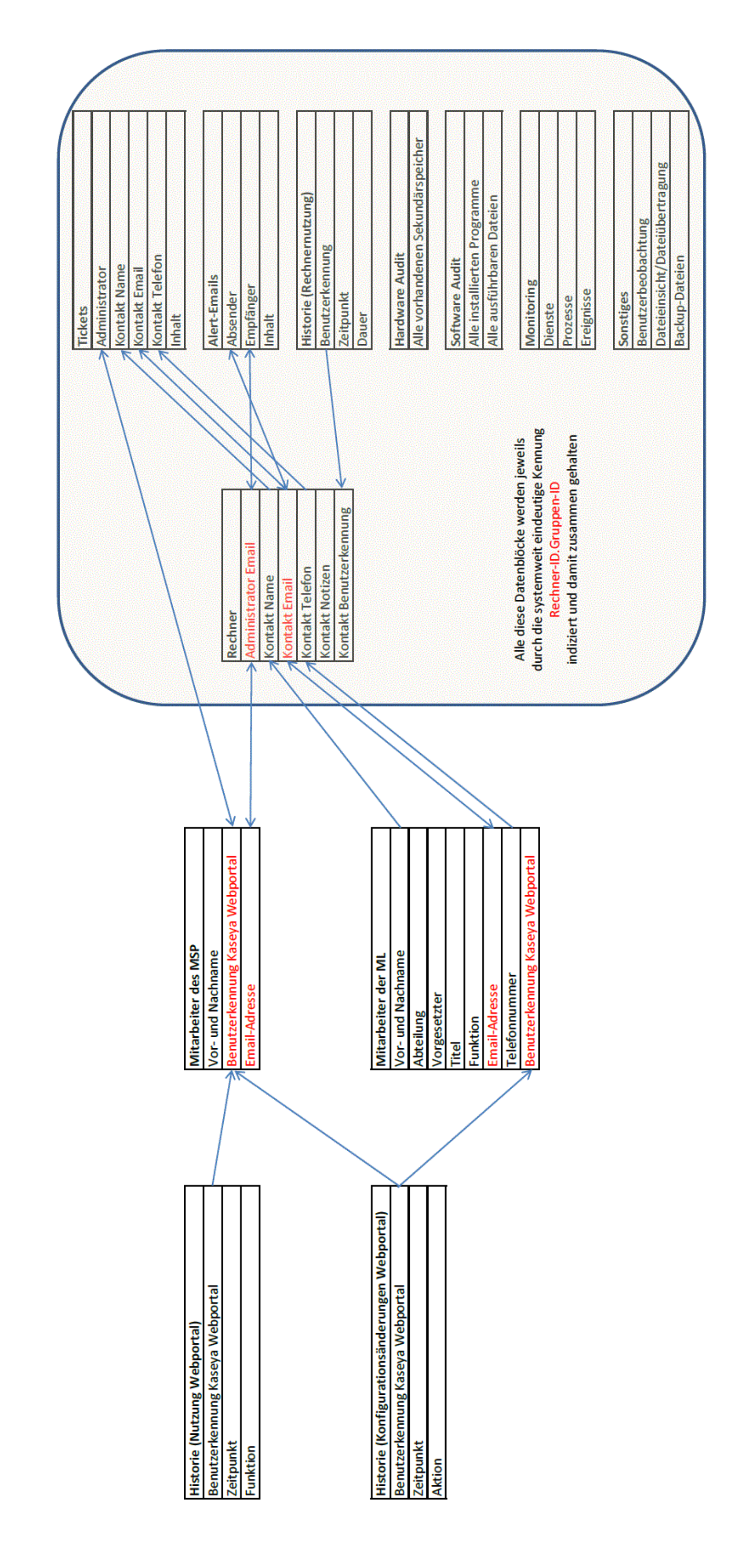


Abbildung 8: Potenzielle Erhebung personenbezogener Daten



SICHERHEITSTEILANALYSE DER VERSION MSE K2 NACH IT-GRUNDSCHUTZ

Mit der Kenntnis, wo und wie personenbezogene Daten beim Einsatz des Kaseya IT Automation Framework auftreten, war zu prüfen, welche datenschutzrechtlichen Konsequenzen sich daraus ergeben.

Dazu erfolgten auf Basis dieser Informationen zunächst eine Teil-Schutzbedarfsfeststellung und anschließend eine Teil-Modellierung nach IT-Grundschutz, wobei neben den Bausteinen der aktuellen IT-Grundschutz-Kataloge auch der Baustein B1.5-Datenschutz-2008-08-26 des BfDI verwendet wurde.

Die Ergebnisse der Teil-Modellierung lieferten auf Basis von realistischen Gefährdungslagen gestaffelte Vorschläge für Maßnahmen, die einen datenschutzkonformen Betrieb der Version MSE K2 gestatten. Bei der nachfolgenden Darstellung werden folglich nur die Gefährdungen bzw. Maßnahmen betrachtet und im Auszug dargestellt, die den Datenschutz beim Einsatz der Version MSE K2 betreffen bzw. fördern[27].

Die dementsprechend als wesentlich identifizierten Bausteine sind in der folgenden Tabelle wiedergegeben:

Tabelle 30: Anwendbare Bausteine IT-Grundschutz, die den Datenschutz betreffen bzw. fördern

Übergeordnete Aspekte	
B 1.14	*Patch- und Änderungsmanagement*
B 1.5	*Datenschutz BfDI*
IT-Infrastruktur	
B 2.1	*Gebäude*
B 2.2	*Elektrotechnische Verkabelung*
B 2.3	*Büroraum*
B 2.4	*Serverraum*
IT-Systeme	
B 3.101	*Allgemeiner Server*
B 3.108	*Windows Server 2003*
B 3.201	*Allgemeiner Client*
B 3.203	*Laptop*
B 3.204	*Client unter Unix*
B 3.209	*Client unter Windows XP*
B 3.301	*Sicherheitsgateway (Firewall)*
B 3.302	*Router und Switches*
IT-Anwendungen	
B 5.4	*Webserver*
B 5.7	*Datenbanken*
B 5.10	*Internet Information Server*

Die in den Bausteinen vorgeschlagenen Maßnahmen werden – soweit für den Datenschutzaspekt notwendig – hinsichtlich besonders relevanter Inhalte im Folgenden in Auszügen wieder gegeben.

---

[27] Daher der Titel „Sicherheitsteilanalyse …“. Eine vollständige Analyse kann und sollte im Rahmen eines Gutachtens zur Datensicherheit der Version MSE K2 erfolgen.



ÜBERGEORDNETE ASPEKTE

M 2.110 DATENSCHUTZASPEKTE BEI DER PROTOKOLLIERUNG (AUSZUG)

Unter Protokollierung beim Betrieb von IT-Systemen ist im datenschutzrechtlichen Sinn die Erstellung von manuellen oder automatisierten Aufzeichnungen zu verstehen, aus denen sich die Fragen beantworten lassen: "Wer hat wann mit welchen Mitteln was veranlasst bzw. worauf zugegriffen?" Außerdem müssen sich Systemzustände ableiten lassen: "Wer hatte von wann bis wann welche Zugriffsrechte?"

Die Effektivität der Protokollierung und ihre Auswertung im Rahmen von Kontrollen hängen im entscheidenden Maße von den technischen und organisatorischen Rahmenbedingungen ab. In diesem Zusammenhang sollten folgende Aspekte Berücksichtigung finden:

- Es sollte ein Revisionskonzept erstellt werden, das den Zweck der Protokolle und deren Kontrollen sowie Schutzmechanismen für die Rechte der Mitarbeiter und der sonstigen betroffenen Personen klar definiert.
- Die Zwangsläufigkeit und damit die Vollständigkeit der Protokolle muss ebenso gewährleistet werden wie die Manipulationssicherheit der Einträge in Protokolldateien.
- Entsprechend der Zweckbindung der Datenbestände müssen wirksame Zugriffsbeschränkungen realisiert werden.
- Die Protokolle müssen so gestaltet sein, dass eine effektive Überprüfung möglich ist. Dazu gehört auch eine IT-Unterstützung der Auswertung.
- Die Auswertungsmöglichkeiten sollten vorab abgestimmt und festgelegt sein.
- Kontrollen sollten so zeitnah durchgeführt werden, dass bei aufgedeckten Verstößen noch Schäden abgewendet sowie Konsequenzen gezogen werden können. Kontrollen müssen rechtzeitig vor dem Ablauf von Löschungsfristen von Protokolldateien stattfinden.
- Kontrollen sollten nach dem 4-Augen-Prinzip erfolgen.
- Es sollte vorab definiert werden, welche Konsequenzen sich aus Verstößen ergeben, die durch die Kontrolle von Protokollen aufgedeckt werden.
- Die Mitarbeiter sollten darüber informiert sein, dass Kontrollen durchgeführt werden, ggf. auch unangekündigt.
- Für Routinekontrollen sollten automatisierte Verfahren (z. B. watch dogs) verwendet werden.
- Personal- bzw. Betriebsräte sollten bei der Erarbeitung des Revisionskonzeptes und bei der Festlegung der Auswertungsmöglichkeiten der Protokolle beteiligt werden.

M 2.23 HERAUSGABE EINER PC-RICHTLINIE (AUSZUG)

Um einen sicheren und ordnungsgemäßen Einsatz von Informationstechnik in größeren Unternehmen bzw. Behörden zu fördern, sollte eine Richtlinie erstellt werden, in der verbindlich vorgeschrieben wird, welche Randbedingungen eingehalten werden müssen und welche IT-Sicherheitsmaßnahmen zu ergreifen sind. Die Richtlinie ist allen Benutzern zur Kenntnis zu geben, beispielsweise in elektronischer Form auf einem Intranet-Server. Jeder neue Benutzer muss die Kenntnisnahme der Richtlinie bestätigen, bevor er die Informationstechnik nutzen darf. Nach größeren Änderungen an der Richtlinie oder nach spätestens 2 Jahren ist eine erneute Bestätigung erforderlich.

Im Folgenden soll grob umrissen werden, welche Inhalte für eine solche Richtlinie sinnvoll sind:

Zielsetzung und Begriffsdefinitionen

Der erste Teil der Richtlinie dient dazu, die Anwender für IT-Sicherheit zu sensibilisieren und zu motivieren. Gleichzeitig werden die für das gemeinsame Verständnis notwendigen Begriffe definiert, wie z. B. PC, Server, Netz, Anwender, Benutzer, schutzbedürftige Objekte.



Geltungsbereich

In diesem Teil muss verbindlich festgelegt werden, für welche Teile des Unternehmens bzw. der Behörde die Richtlinie gilt.

Rechtsvorschriften und interne Regelungen

Hier wird im Überblick dargestellt, welche wesentlichen Rechtsvorschriften, z. B. das Bundesdatenschutzgesetz und das Urheberrechtsgesetz, einzuhalten sind. Anhand von Beispielen sollte deutlich gemacht werden, welche Auswirkungen dies auf die Nutzung der Informationstechnik im jeweiligen Umfeld hat. Darüber hinaus kann diese Stelle genutzt werden, um alle relevanten betriebsinternen Regelungen aufzuführen.

Verantwortungsverteilung

In diesem Teil wird definiert, welcher Funktionsträger im Zusammenhang mit dem IT-Einsatz welche Verantwortung tragen muss. Dabei sind insbesondere die Rollen Benutzer, Vorgesetzte, Administrator, Revisor, Datenschutzbeauftragter und IT-Sicherheitsmanagement-Team zu unterscheiden.

Ansprechpartner

Die Richtlinie sollte Ansprechpartner und Kontaktinformationen (Telefon, E-Mail etc.) für die Benutzer zu Fragen der IT-Sicherheit enthalten oder aufzeigen, wo diese Informationen gefunden werden können. Dabei sollte beachtet werden, dass es häufig zu Verwirrung führt, wenn den Benutzern zu viele unterschiedliche Ansprechpartner genannt werden. Besser ist es meist, nur wenige unterschiedliche Ansprechpartner zu benennen, die dann bei Bedarf die Benutzer an die richtige Stelle verweisen (Help-Desk-Konzept).

Umzusetzende und einzuhaltende IT-Sicherheitsmaßnahmen

Im letzten Teil der Richtlinie für die IT-Nutzung ist festzulegen, welche IT-Sicherheitsmaßnahmen vom Benutzer einzuhalten bzw. umzusetzen sind. Dies kann je nach Schutzbedarf auch über die IT-Grundschutz-Maßnahmen hinausgehen. Typische Beispiele für IT-Sicherheitsmaßnahmen am Arbeitsplatz sind das sichere An- und Abmelden am PC, der ordnungsgemäße Umgang mit Passwörtern und Verhaltensregeln bei der Nutzung des Internets.

M 2.424 SICHERHEITSRICHTLINIE ZUM EINSATZ VON PATCH- UND ÄNDERUNGSMANAGEMENT-WERKZEUGEN (AUSZUG)

Ein Patch- und Änderungsmanagement-Werkzeug spielt als zentrale Instanz zur Umsetzung des Patch- und Änderungsmanagementprozesses und zur Softwareverteilung für den sicheren und ordnungsgemäßen Betrieb der Institution eine wesentliche Rolle.

Das Patch- und Änderungsmanagement muss mit einem angemessenen organisatorischen und technischen Aufwand betrieben werden. Dabei sind unter anderem der Schutzbedarf der Geschäftsprozesse und damit der Schutzbedarf der Daten und Systeme zu berücksichtigen. Dafür sollte eine spezifische Sicherheitsrichtlinie für das Patch- und Änderungsmanagement erstellt werden. Diese muss mit dem Sicherheitskonzept der Institution und den daraus abgeleiteten Sicherheitsrichtlinien abgestimmt sein.

Aspekte, zu denen in dieser Sicherheitsrichtlinie Vorgaben formuliert werden müssen, sind:

Vorgaben für die Planung:

- Zur Skalierbarkeit der Serverapplikation des Werkzeugs müssen bereits im Vorfeld Anforderungen zum Einsatz von Replikation, Lastverteilung und der Möglichkeit, technische Redundanzen zu benutzen, formuliert werden.
- Für eine sichere Netzverbindung zu externen Bezugsquellen von Patches oder Änderungen z. B. bei Herstellern müssen geeignete Regelungen festgelegt werden. Beispielsweise könnte die Direktverbindung der Clients zu den Herstellern der eingesetzten Software durch entsprechende Regeln auf dem Sicherheitsgateway auf einen Proxy umgeleitet werden.
- Damit Integrität und Authentizität von Patches und Änderungen zuverlässig überprüft werden kann, müssen geeignete Konzepte und Komponenten festgelegt werden.
- Es müssen Anforderungen zum Bereitstellen der Dokumentation für Betrieb, Notfall und Wiederanlauf des Patch- und Änderungsmanagement-Werkzeugs formuliert werden. Zu den Anforderungen gehören unter anderem, dass die Dokumentation immer aktuell sein muss. Des Weiteren sollte definiert werden, wo die Dokumentation gelagert werden muss und wie viele Exemplare der Dokumentation vorhanden sein müssen.

Vorgaben für die Administration:

- Es ist erforderlich, ein Rechtekonzept für Mitarbeiter im Patch- und Änderungsmanagement und auch für die Dienste, welche von der Patch- und Änderungsmanagementsoftware verwendet werden, zu erstellen.
- Für die Administratoren ist festzulegen, wie Rechte vergeben werden. welche sie bekommen oder welche sie verteilen dürfen.

Vorgaben für die Installation:

- Die Werkzeuge für das Patch- und Änderungsmanagement müssen sicher konfiguriert werden. Die jeweiligen konkreten Einstellungen hängen stark von den vorhandenen Anwendungen und IT-Systemen der Institution ab. Allgemeine Hinweise hierzu finden sich in M 4.237 Sichere Grundkonfiguration eines IT-Systems.
- Es muss festgelegt werden, wie die für das Patch- und Änderungsmanagement-Werkzeug relevanten IT-Ressourcen, wie beispielsweise die Komponenten der Software zur Verteilung von Patches und Änderungen und der Betriebssysteme unter Berücksichtigung von Sicherheitsaspekten konfiguriert werden.
- Das Patch- und Änderungsmanagement-Werkzeug sollte angemessen im LAN separiert werden. Neue Änderungen und Patches sollten nicht im Produktivnetz getestet werden, sondern in einem separaten Testnetz.

Vorgaben für den sicheren Betrieb:

- Für den Betrieb eines Patch- und Änderungsmanagement-Tools sind Vorgaben und Abläufe festzulegen, also beispielsweise, wer darauf zugreifen darf und wo Änderungen durchgeführt werden dürfen.
- Patches und Änderungen werden häufig über das Internet bezogen. Verbindungen in öffentliche oder weniger vertrauliche Netze sind grundsätzlich über Sicherheitsgateways abzusichern.
- Das Patch- und Änderungsmanagement-Werkzeug selbst muss in den Prozess des Patch- und Änderungsmanagements mit eingegliedert werden. In dem Zusammenhang ist zu definieren, wie Hard- und Software-Änderungen für das Patch- und Änderungsmanagement-Werkzeug selbst zu behandeln sind.

Vorgaben für Protokollierung und Monitoring:

- Die Art und Weise der Überwachung, Protokollierung und der Auswertung der vom Patch- und Änderungsmanagement-Werkzeug gelieferten Daten ist festzulegen

Datensicherung:

Ein geeignetes Verfahren für die Datensicherung ist festzulegen. Bei der Datensicherung sollten mindestens folgende Komponenten in regelmäßigen Abständen gesichert werden:

- Die Konfiguration bzw. die Einstellungen der für das Patch- und Änderungsmanagement benötigten Werkzeuge
- Die Datenbanken mit den aktuellen Konfigurationen der IT-Systeme
- Bei selbstübersetzter Software die genauen Compilier-Einstellungen
- Die installierten Patches und Änderungen
- Die letzten Wiederherstellungspunkte der IT-Systeme
- Eventuell vorhandene ältere Versionsstände, beispielsweise weil die neuste Version einer Software noch nicht ausreichend getestet wurde oder nicht auf allen Systemen lauffähig ist
- Eine Übersicht über die Vergleichsprüfsummen der Softwarepakete, diese sollte eventuell auf einem Write Once Read Many - Medium (WORM) gesichert werden

Störung und Notfallvorsorge:

- Für die Notfallvorsorge müssen die einzelnen Notfallpläne der Anwendungen und IT-Systeme, die vom Patch- und Änderungsmanagement ferngewartet werden, berücksichtigt werden.
- In Abhängigkeit von den Verfügbarkeitsanforderungen an das Patch- und Änderungsmanagement-Werkzeugs sollte überlegt werden, ob für das Patch- und Änderungsmanagement-Werkzeug ein separater Notfallplan für unerwünschte Effekte bei und nach der Installation von Patches und Änderungen erstellt wird.

M 7.12 REGELUNG DER VERKNÜPFUNG UND VERWENDUNG VON DATEN BEI DER VERARBEITUNG PERSONENBEZOGENER DATEN (AUSZUG)

Bevor die sogenannten freien Abfragesprachen im Zusammenhang mit personenbezogener Datenverarbeitung zugelassen werden, muss geprüft werden, ob dies mit der Schutzwürdigkeit der Daten vereinbar ist. Wenn es grundsätzlich vereinbar ist, sollten folgende Anforderungen beachtet werden: Das System muss eine technische Begrenzung aufweisen, ähnlich einem Filter, der sicherstellt, dass die "freie Abfragesprache" nur im vereinbarten Umfang eingesetzt werden kann. Der Umfang kann beispielsweise durch eine Zugriffsbeschränkung auf bestimmte, weniger sensitive Datenfelder festgelegt sein. Ein Umgehen des Filters ist insbesondere programmtechnisch zu verhindern.

Die Daten, auf die mit einer solchen Abfragesprache zugegriffen werden soll, und die zu eröffnenden Abfragearten müssen vorab geprüft werden. Kriterien sind hierbei insbesondere

- die Erforderlichkeit für die Aufgabenerfüllung,
- der Nachweis, dass eine anonymisierte Auswertung für den jeweils verfolgten Zweck nicht genügt,
- die Sensibilität der einzelnen Daten in der vorgesehenen Verknüpfung und Systemumgebung sowie
- der jeweilige Zweck und Kontext der Datennutzung.

Keine datenschutzrechtlichen Bedenken bestehen gegen den Einsatz einer "freien Abfragesprache" dann, wenn die Auswertung nur zu anonymisierten Ergebnissen führt, d. h. Rückschlüsse auf einzelne Personen nicht möglich sind.

IT-INFRASTRUKTUR

M 1.10 VERWENDUNG VON SICHERHEITSTÜREN UND –FENSTERN (AUSZUG)

Der Einsatz von Sicherheitstüren ist hinsichtlich der Brandschutzes über den von der Bauaufsicht und der Feuerwehr vorgeschriebenen Bereich hinaus (siehe M 1.6 Einhaltung von Brandschutzvorschriften) besonders bei schutzbedürftigen Räumen wie Serverraum, Beleg- oder Datenträgerarchiv sinnvoll. Bei hochschutzbedürftigen Räumen ist ein ausgewogenes Schutzkonzept zu erstellen, welches den Einbau von Sicherheitstüren und die Gefahrenmeldung und Alarmierung zur Prüfung und Intervention berücksichtigt.

Es ist dafür zu sorgen, dass Brand- und Rauchschutztüren auch tatsächlich geschlossen und nicht (unzulässigerweise) z. B. durch Keile offen gehalten werden. Alternativ können Türen mit einem automatischen Schließmechanismus, der im Alarmfall aktiviert wird, eingesetzt werden.

M 1.12 VERMEIDUNG VON LAGEHINWEISEN AUF SCHÜTZENSWERTE GEBÄUDETEILE (AUSZUG)

Schützenswerte Gebäudeteile sind z. B. Serverraum, Rechenzentrum, Datenträgerarchiv, Klimazentrale, Verteilungen der Stromversorgung, Schalt- und Rangierräume, Ersatzteillager.

Solche Bereiche sollten keinen Hinweis auf ihre Nutzung tragen. Türschilder wie z. B. RECHENZENTRUM oder EDV-ARCHIV geben einem potentiellen Angreifer, der zum Gebäude Zutritt hat, Hinweise, um seine Aktivitäten gezielter und damit Erfolg versprechender vorbereiten zu können.

Ist es unvermeidbar, IT in Räumen oder Gebäudebereichen unterzubringen, die für Fremde leicht von außen einsehbar sind (siehe auch M 1.13 Anordnung schützenswerter Gebäudeteile), so sind geeignete Maßnahmen zu treffen, um den Einblick zu verhindern oder so zu gestalten, dass die Nutzung nicht offenbar wird. Dabei ist darauf zu achten, dass z. B. nicht nur ein Fenster einer ganzen Etage mit einem Sichtschutz versehen wird.

M 1.15 GESCHLOSSENE FENSTER UND TÜREN (AUSZUG)

Fenster und nach außen gehende Türen (Balkone, Terrassen) müssen in Zeiten, in denen ein Raum nicht besetzt ist, geschlossen werden. Außentüren sind abzuschließen. Im Keller- und Erdgeschoss und, je nach Fassadengestaltung, auch in den höheren Etagen, bieten offene Fenster und Türen Einbrechern ideale Einstiegsmöglichkeiten, die auch während der Betriebszeiten einer Institution genutzt werden.

M 1.18 GEFAHRENMELDEANLAGE (AUSZUG)

Eine Gefahrenmeldeanlage (GMA) besteht aus einer Vielzahl lokaler Melder, die mit einer Zentrale kommunizieren, über die auch der Alarm ausgelöst wird. Ist eine Gefahrenmeldeanlage für Einbruch, Brand, Wasser oder auch Gas vorhanden und lässt sich diese mit vertretbarem Aufwand entsprechend erweitern, sollten zumindest die Kernbereiche der IT (Serverräume, Datenträgerarchive, Räume für technische Infrastruktur u. ä.) in die Überwachung durch diese Anlage mit eingebunden werden. So lassen sich Gefährdungen wie Feuer, Einbruch, Diebstahl frühzeitig erkennen und Gegenmaßnahmen einleiten. Um dies zu gewährleisten, ist die Weiterleitung der Meldungen an eine ständig besetzte Stelle (Pförtner, Wach- und Sicherheitsdienst, Feuerwehr, etc.) unumgänglich. Dabei muss sichergestellt sein, dass diese Stelle auch in der Lage ist, technisch und personell auf den

Alarm zu reagieren.

M 1.23 ABGESCHLOSSENE TÜREN (AUSZUG)

Die Türen nicht besetzter Räume sollten abgeschlossen werden. Dadurch wird verhindert, dass Unbefugten Zugriff auf darin befindliche Unterlagen und IT-Einrichtungen erlangen. Das Abschließen einzelner Büros ist insbesondere dann wichtig, wenn sich diese in Bereichen mit Publikumsverkehr befinden oder der Zutritt nicht durch andere Maßnahmen kontrolliert wird.

M 1.27 KLIMATISIERUNG (AUSZUG)

Um IT-Geräte dauerhaft zuverlässig zu betreiben, muss sichergestellt werden, dass die Umgebungsbedingungen innerhalb der von den Herstellern genannten Grenzen gehalten werden. Der in diesem Zusammenhang stets genutzte Begriff Klimatisierung umfasst die folgenden vier Bereiche der Luftkonditionierung:

- Lufttemperatur
- Luftfeuchtigkeit
- Frischluftanteil
- Schwebstoffbelastung

M 1.28 LOKALE UNTERBRECHUNGSFREIE STROMVERSORGUNG (AUSZUG)

Eine lokale unterbrechungsfreien Stromversorgung (USV) hat die Aufgabe, ein einzelnes IT-System oder sehr wenige IT-Geräte gegen die Folgen kurzfristiger Unterbrechungen der Stromversorgung zu schützen. Diese Zielsetzung ist meist in kleineren IT-Strukturen gegeben, die zudem nicht über eine Netzersatzanlage verfügen.

Für größere IT-Strukturen oder gar die Versorgung ganzer Gebäude werden vornehmlich zentrale USV-Systeme eingesetzt (siehe M 1.70 Zentrale unterbrechungsfreie Stromversorgung).

M 1.58 TECHNISCHE UND ORGANISATORISCHE VORGABEN FÜR SERVERRÄUME (AUSZUG)

Ein Serverraum sollte als geschlossener Sicherheitsbereich konzipiert sein. Dieser sollte möglichst gut zu sichernde Zugangstüren und Fenster haben, da alle Zutrittsmöglichkeiten überwacht werden müssen (siehe auch M 1.10 Verwendung von Sicherheitstüren und -fenstern). Der Zutritt sollte durch hochwertige Zutrittskontrollmechanismen geschützt werden. Bei der Planung eines Serverraumes bzw. der Auswahl geeigneter Räumlichkeiten sollten potentielle Gefährdungen durch Umgebungseinflüsse möglichst minimiert werden.

M 2.14 SCHLÜSSELVERWALTUNG (AUSZUG)

Für alle Schlüssel des Gebäudes (von Etagen, Fluren und Räumen) ist ein Schließplan zu fertigen. Die Herstellung, Aufbewahrung, Verwaltung und Ausgabe von Schlüsseln ist zentral zu regeln. Reserveschlüssel sind vorzuhalten und gesichert aufzubewahren. Das gleiche gilt auch für alle Identifikationsmittel wie Magnetstreifen- oder Chipkarten.

M 2.17 ZUTRITTSREGELUNG UND -KONTROLLE

Der Zutritt zu schutzbedürftigen Gebäudeteilen und Räumen ist zu regeln und zu kontrollieren (siehe M 2.6 Vergabe von Zutrittsberechtigungen). Die Maßnahmen reichen dabei von einer einfachen Schlüsselvergabe bis zu aufwendigen Identifizierungssystemen mit Personenvereinzelung, wobei auch die Nutzung eines mechani-

schen Schlüssels nebst Schloss eine Zutrittsregelung darstellt.

Die Vergabe von Rechten allein reicht nicht aus, wenn deren Einhaltung bzw. Überschreitung nicht kontrolliert wird. Die Ausgestaltung von Kontrollmechanismen sollte nach dem Grundsatz erfolgen, dass einfache und praktikable Lösungen oft ebenso effizient sind wie aufwendige Technik.

Bei der Zutrittskontrolle werden verschiedene bauliche, organisatorische und personelle Maßnahmen benötigt. Deren Zusammenwirken sollte in einem Zutrittskontrollkonzept geregelt sein, das die generellen Richtlinien für den Perimeter-, Gebäude- und Geräteschutz festlegt.

Zu schützende Bereiche können etwa Grundstücke, Gebäude, Serverräume, Räume mit Peripheriegeräten, Archive, Kommunikationseinrichtungen und die Haustechnik sein. Da diese Bereiche häufig sehr unterschiedliche Sicherheitsanforderungen aufweisen, kann es sinnvoll sein, diese in verschiedene Sicherheitszonen aufzuteilen.

Die Terminals zur Zutrittskontrolle müssen gegen Manipulationen geschützt werden. Dafür müssen diese so angebracht werden, dass Vertraulichkeit bei der Eingabe von Daten gewährleistet ist. Außerdem sollten alle zur Dateneingabe erforderlichen Einheiten in einem Gerät kombiniert sein, also beispielweise eine Tastatur zur PIN-Eingabe.

Befinden sich nicht alle Einheiten in einem Gerät, muss die Datenübertragung zwischen diesen verschlüsselt erfolgen. Werden also z. B. berührungslose Ausweisleser eingesetzt, so muss die Datenübertragung zwischen Karte und Leser verschlüsselt erfolgen.

M 2.21 RAUCHVERBOT

In Räumen mit IT oder Datenträgern (Serverraum, Datenträgerarchiv, aber auch Belegarchiv), in denen Brände oder Verschmutzungen zu hohen Schäden führen können, sollte ein Rauchverbot erlassen werden. Dieses Rauchverbot dient gleicherweise dem vorbeugenden Brandschutz wie der Betriebssicherheit von IT mit mechanischen Funktionseinheiten.

IT-SYSTEME

M 1.46 EINSATZ VON DIEBSTAHL-SICHERUNGEN (AUSZUG)

Diebstahl-Sicherungen sind überall dort einzusetzen, wo große Werte zu schützen sind bzw. dort, wo andere Maßnahmen - z. B. geeignete Zutrittskontrolle zu den Arbeitsplätzen - nicht umgesetzt werden können, wie etwa bei Laptops im mobilen Einsatz. Diebstahl-Sicherungen machen außerdem dort Sinn, wo Publikumsverkehr herrscht oder die Fluktuation von Benutzern sehr hoch ist. Dabei sollte immer bedacht werden, dass die zu schützenden Werte nur zu einem kleinen Teil aus den Wiederbeschaffungskosten für das Gerät bestehen, sondern bei Laptops und ähnlichen IT-Systemen der Wert der darauf gespeicherten Daten berücksichtigt werden muss.

M 2.218 REGELUNG DER MITNAHME VON DATENTRÄGERN UND IT-KOMPONENTEN (AUSZUG)

Die IT-Komponenten, die innerhalb einer hauseigenen Liegenschaft eingesetzt werden, sind im Allgemeinen durch infrastrukturelle Sicherheitsmaßnahmen ausreichend vor Missbrauch und Diebstahl geschützt. Häufig sollen aber IT-Systeme oder Datenträger auch außer Haus eingesetzt werden, z. B. bei Dienstreisen oder Telearbeit. Um auch diese ausreichend schützen zu können, muss die Mitnahme von Datenträgern und IT-

Komponenten klar geregelt werden.

M 2.309 SICHERHEITSRICHTLINIEN UND REGELUNGEN FÜR DIE MOBILE IT-NUTZUNG (AUSZUG)

IT-Systeme, die außerhalb der eigenen Institution eingesetzt werden, sind mehr Risiken ausgesetzt, als solche, die sich innerhalb geschützter Räumlichkeiten befinden. Trotzdem gibt es eine Vielzahl von Möglichkeiten, mobile IT-Systeme unterwegs zu schützen. Damit diese Möglichkeiten auch genutzt werden, sollte eine Sicherheitsrichtlinie erstellt werden, in der alle umzusetzenden Sicherheitsmechanismen beschrieben sind. Zusätzlich sollte für die Benutzer ein kurzes und übersichtliches Merkblatt für die sichere Nutzung von mobilen IT-Systemen erstellt werden.

- Die Benutzer müssen darüber informiert sein, welche Informationen mit mobilen IT-Systemen unterwegs verarbeitet werden dürfen. Die Daten sollten dementsprechend klassifiziert sein, um Einschränkungen den Benutzern transparent zu machen (siehe auch M 2.217 Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen). Dienstgeheimnisse dürfen nur dann auf mobilen IT-Systemen verarbeitet werden, wenn hierfür geeignete und freigegebene Sicherheitsmechanismen eingesetzt werden.
- Daten, die ein hohes Maß an Sicherheit verlangen (z.B. Angebote, Konstruktionsdaten, Wirtschaftsdaten des Unternehmens) sollten stets verschlüsselt auf dem mobilen IT-System abgelegt werden.
- Beim Einsatz mobiler IT-Systeme ist zu klären, ob mobile Mitarbeiter von unterwegs Zugriff auf interne Daten ihrer Institution erhalten.
- Falls dies vorgesehen ist, muss dieser Zugriff angemessen geschützt werden (siehe hierzu auch M 5.121 Sichere Kommunikation von unterwegs und M 5.122 Sicherer Anschluss von Laptops an lokale Netze).
- Es muss geklärt werden, ob diese auch für private Zwecke benutzt werden dürfen, beispielsweise für private Schreiben oder ein Spielchen nach Feierabend.
- Die Benutzer sollten darauf hingewiesen werden, wie sie sorgfältig mit den mobilen IT-Systemen umgehen sollten, um einem Verlust oder Diebstahl vorzubeugen bzw. um eine lange Lebensdauer zu gewährleisten (z. B. Akkupflege, Aufbewahrung außerhalb von Büro- oder Wohnräumen, Empfindlichkeit gegenüber zu hohen oder zu niedrigen Temperaturen).
- Die Verwaltung, Wartung und Weitergabe von mobilen IT-Systemen sollte geregelt werden.
- Bei jedem Benutzerwechsel müssen alle benötigten Passwörter gesichert weitergegeben werden (siehe M 2.22 Hinterlegen des Passwortes).

M 3.18 VERPFLICHTUNG DER BENUTZER ZUM ABMELDEN NACH AUFGABENERFÜLLUNG (AUSZUG)

Wird ein IT-System oder eine IT-Anwendung von mehreren Benutzern verwendet und besitzen die einzelnen Benutzer unterschiedliche Zugriffsrechte auf dort gespeicherte Daten oder Programme, so kann der erforderliche Schutz mittels einer Zugriffskontrolle nur dann erreicht werden, wenn jeder Benutzer sich nach Aufgabenerfüllung am IT-System oder der IT-Anwendung abmeldet. Ist es einem Dritten möglich, an einem IT-System oder in einer IT-Anwendung unter der Identität eines anderen weiterzuarbeiten, so ist jegliche sinnvolle Zugriffskontrolle unmöglich. Daher sind alle Benutzer zu verpflichten, sich nach Aufgabenerfüllung vom IT-System bzw. von der IT-Anwendung abzumelden. Aus technischen Gründen (z. B. damit alle offenen Dateien geschlossen werden) sollten auch dann Regelungen für die Abmeldung von IT-Systemen und IT-Anwendungen getroffen werden, wenn keine Zugriffskontrolle realisiert ist.

M 4.279 ERWEITERTE SICHERHEITSASPEKTE FÜR WINDOWS SERVER 2003 (AUSZUG)

Bei hohen Verfügbarkeitsanforderungen kann es erforderlich sein, nicht nur Teile der Serverhardware, sondern den gesamten Server redundant auszulegen und in einem Hochverfügbarkeits-Cluster zusammenzufassen. Windows Server 2003 Enterprise Edition unterstützt mittels des Clusterdienstes acht Knoten in einem Cluster, die je nach Anforderung für Hochverfügbarkeit und Lastverteilung optimiert werden können. Jeder der redundanten Server sollte einheitlichen Hardwareanforderungen gerecht werden. Die Planung des Clusters muss bei der Rollenplanung berücksichtigt werden, da bestimmte Dienste nur eingeschränkt clusterfähig sind. Der Netzwerklastenausgleich wird nicht nur von der Enterprise Edition, sondern auch von der Web Edition und der Standard Edition unterstützt.

M 4.48 PASSWORTSCHUTZ UNTER NT-BASIERTEN WINDOWS-SYSTEMEN (AUSZUG)

Die Anforderungen an Passwörter unter NT-basierten Windows-Systemen sollten dokumentiert werden, gegebenenfalls in Form einer Sicherheitsrichtlinie. Die Dokumentation bzw. Richtlinie sollte die Einstellungen der folgenden Tabelle umfassen. Die letzte Spalte enthält Mindestempfehlungen für normalen Schutzbedarf:

Tabelle 31: Empfohlene Anforderungen an Passwörter unter Windows

Windows NT	Windows 2000/XP/2003	Windows Vista	
Maximales Kennwortalter	Maximales Kennwortalter	Maximales Kennwortalter	90 Tage
Minimales Kennwortalter	Minimales Kennwortalter	Minimales Kennwortalter	1 Tag
Minimale Kennwortlänge	Minimale Kennwortlänge	Minimale Kennwortlänge	8 Zeichen
Kennwortzyklus	Kennwortchronik erzwingen	Kennwortchronik erzwingen	6 Kennwörter
Konto sperren | Sperren nach	Kontosperrungsschwelle	Kontosperrungsschwelle	3 Versuchen
Konto sperren | Konto zurücksetzen nach	Zurücksetzungsdauer des Kontosperrungszählers	Zurücksetzungsdauer des Kontosperrungszählers	30 Minuten
Dauer der Sperrung	Kontosperrdauer	Kontosperrdauer	60 Minuten
Benutzer muss sich anmelden, um Kennwort zu ändern	n/v	n/v	Deaktiviert
n/v	Kennwort muss Komplexitätsvoraussetzungen entsprechen	Kennwort muss Komplexitätsvoraussetzungen entsprechen	Aktiviert
n/v	Kennwörter für alle Domänenbenutzer mit umkehrbarer Verschlüsselung speichern	Kennwörter mit umkehrbarer Verschlüsselung speichern	Deaktiviert

IT-ANWENDUNGEN

M 2.128 ZUGANGSKONTROLLE EINER DATENBANK (AUSZUG)

Die Datenbank-Software muss über geeignete Mechanismen zur Identifikation und Authentisierung der Benutzer verfügen, um eine wirkungsvolle Zugangskontrolle zu gewährleisten. Die Vergabe von Zugangsberechtigungen hat nach festgelegten Regeln zu erfolgen (siehe M 2.132 Regelung für die Einrichtung von Datenbankbenutzern/-benutzergruppen).

Generell sollte für normale Benutzer der Zugang zu einer Produktionsdatenbank über einen interaktiven SQL-Interpreter unterbunden werden. Auf solche Datenbanken sollte ausschließlich ein indirekter Zugang über die entsprechenden Anwendungen möglich sein. Die einzige Ausnahme bilden hier Datenbankkennungen zu Administrationszwecken.

M 2.174 SICHERER BETRIEB EINES WEBSERVERS (AUSZUG)

WWW-Server sind attraktive Ziele für Angreifer und müssen daher sehr sorgfältig konfiguriert werden, damit sie sicher betrieben werden können. Das Betriebssystem und die Software müssen so konfiguriert sein, dass der Rechner so gut wie möglich gegen Angriffe geschützt wird. Solange der Rechner nicht entsprechend konfiguriert ist, darf er nicht ans Netz genommen werden.

Daher sollte ein WWW-Server, der Informationen im Internet anbietet, entsprechend den folgenden Vorgaben installiert werden:

- Auf einem WWW-Server sollte nur ein Minimum an Programmen vorhanden sein, d. h. das Betriebssystem sollte auf die unbedingt erforderlichen Funktionalitäten reduziert werden und auch sonst sollten sich nur unbedingt benötigte Programme auf dem WWW-Server befinden (siehe M 4.95 Minimales Betriebssystem).
- Ein WWW-Server sollte insbesondere keine unnötigen Netzdienste enthalten, verschiedene Dienste gehören auf verschiedene Rechner (siehe M 4.97 Ein Dienst pro Server).
- Der Zugriff auf Dateien oder Verzeichnisse muss geschützt werden (siehe M 4.94 Schutz der WWW-Dateien).
- Die Kommunikation mit dem WWW-Server sollte durch einen Paketfilter auf ein Minimum beschränkt werden (siehe M 4.98 Kommunikation durch Paketfilter auf Minimum beschränken).
- Die Administration des WWW-Servers darf nur über eine sichere Verbindung erfolgen, d. h. die Administration sollte an der Konsole direkt, nach starker Authentisierung (bei Zugriff aus dem LAN) oder über eine verschlüsselte Verbindung (bei Zugriff aus dem Internet) erfolgen.
- Weiterhin sollte der WWW-Server vor dem Internet durch einen Firewall-Proxy oder aber zumindest durch einen Paketfilter (siehe M 4.98 Kommunikation durch Paketfilter auf Minimum beschränken) abgesichert werden. Er darf sich nicht zwischen Firewall und internem Netz befinden, da ein Fehler auf dem WWW-Server sonst Zugriffe auf interne Daten ermöglichen könnte.

M 2.268 FESTLEGUNG EINER IIS-SICHERHEITSRICHTLINIE

Für den Einsatz von IIS ist eine geeignete Sicherheitsrichtlinie zu definieren. In der Sicherheitsrichtlinie muss festgelegt werden, was zu unternehmen ist, um ein System effektiv abzusichern.

Zugriffsregeln

In der Sicherheitsrichtlinie müssen folgende Zugriffsregeln festgelegt werden:

- Welcher Benutzer darf auf welchen Server zugreifen und welche Benutzer sollen auf welchen Server nicht zugreifen (Ausschlussliste)?
- Welcher Benutzer darf auf welche Verzeichnisse und Web-Seiten zugreifen bzw. nicht zugreifen (Ausschlussliste)?
- Welche Authentisierung ist zum Zugriff auf Verzeichnisse und Web-Seiten erforderlich?
- Welche Anwendungen und Scripts werden mit welchen Rechten ausgeführt?
- Wie und mit welchen Rechten darf auf angeschlossene Datenbanken zugegriffen werden?
- Von wo aus darf auf den IIS zugegriffen werden?

Verschlüsselung und Signatur

Außerdem muss festgelegt werden, ob eine Kommunikationsabsicherung, z. B. SSL, eingesetzt werden soll, welcher Mechanismus genutzt wird und welche Kommunikationsverbindungen geschützt werden sollen.

Audit und Protokollierung

Es muss ein Auditing- und Protokollierungskonzept entworfen werden. Es ist darauf zu achten, dass der Datenschutzbeauftragte in die Planung mit einbezogen wird, da im Rahmen der Überwachung auch personenbezogene Daten anfallen können.

M 4.278 SICHERE NUTZUNG VON EFS UNTER WINDOWS SERVER 2003 (AUSZUG)

Das verschlüsselnde Dateisystem (Encrypting File System, EFS) von Windows Server 2003/XP ist für Benutzer ein einfach zu bedienendes Mittel zum anwendungsunabhängigen Arbeiten mit verschlüsselten Dateien. Es eignet sich am besten für einzelne Benutzer und exponierte Client-Computer, die zeitweise außerhalb der geschützten IT-Umgebung zum Einsatz kommen. Die Hauptintention ist das Herstellen von Vertraulichkeit für dedizierte lokale Daten. Grundlagen sind M 4.147 Sichere Nutzung von EFS unter Windows zu entnehmen.

Weniger geeignet ist EFS für die großflächige Verschlüsselung von zentralisierten Benutzerdaten auf Remote-Servern, beispielsweise Dateiservern. Dies ist nur mit spezieller Planung der Schlüsselverwaltung zu realisieren. Einen erheblichen Aufwand für die Sicherung und den Schutz großer Datenmengen und einer Vielzahl von Benutzerschlüsseln muss in Kauf genommen werden.

M 4.72 DATENBANK-VERSCHLÜSSELUNG (AUSZUG)

In Abhängigkeit von der Art der in einer Datenbank gespeicherten Informationen und den sich daraus ergebenden Anforderungen an deren Vertraulichkeit und Integrität kann es notwendig werden, diese Daten zu verschlüsseln.

Welche Daten mit welchem Verfahren zu verschlüsseln sind, ist am besten bereits bei der Auswahl der Datenbank-Standardsoftware festzustellen (siehe M 2.124 Geeignete Auswahl einer Datenbank-Software). Dabei sollten die Anforderungen hinsichtlich der Verschlüsselung von Datenbeständen mit den entsprechenden Leistungsmerkmalen der Datenbank-Software verglichen werden. Als Mindestanforderung sollte sie in jedem Fall sicherstellen, dass die Passwörter der Benutzer-Kennungen der Datenbank verschlüsselt abgelegt sind.

Falls die Anforderungen durch keine der am Markt verfügbaren Datenbank-Standardsoftware abgedeckt werden können, sollte man den Einsatz von Zusatzprodukten prüfen, um die entsprechende Sicherheitslücke zu schließen. Falls auch keine Zusatzprodukte erhältlich sind, muss ein Konzept für die Umsetzung einer Verschlüsselungsstrategie erstellt werden, das im Unternehmen bzw. in der Behörde umgesetzt wird.

DATENSCHUTZRECHTLICHE ANALYSE DER VERSION MSE K2

Im Anschluss an die Sicherheitsteilanalyse wurden die wichtigsten Implikationen der Gesetzeswerke BDSG, TMG, TKG und StGB ermittelt. Berücksichtigt wurden dabei u.a. auch

- der Anforderungskatalog v 1.2 für die Begutachtung von IT-Produkten im Rahmen des Gütesiegelverfahrens beim ULD SH und
- der Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich vom 26./27. November 2009 in Stralsund (hinsichtlich Web-Analysen).

IMPLIKATIONEN DES BDSG

Da der Einsatz der Version MSE K2 für das Verfahren der Fernwartung/Fernbetreuung einen Zugriff auf personenbezogene Daten der Mitarbeiter im Hause ML regelmäßig einschließt, liegt nach § 11 (5) BDSG eine Auftragsdatenverarbeitung (ADV) zumindest für den Bereich Fernwartung vor.

Dies bedeutet, dass die ML verantwortliche Stelle (§ 3 (7) BDSG) bleibt. Der MSP ist im Bereich Fernwartung nur ein unselbständiger Handlanger. Deshalb darf der MSP alle Daten, die er bei der ML erhebt, auch nur nach den von der ML festzulegenden Vorgaben verarbeiten. Insbesondere muss die ML die Datenerhebung, Datenverarbeitung oder Datennutzung, die technischen und organisatorischen Maßnahmen und etwaige Unterauftragsverhältnisse zumindest im Bereich Fernwartung schriftlich vollständig für den MSP festlegen.

Die ML alleine trägt zunächst die Verantwortung für die korrekte Fernwartung, auch wenn sie die Aufgaben an sich an den MSP vergibt. Es sind im entsprechenden Vertrag also genaue Vorgaben zu machen. So ist beispielsweise zu klären, wann genau ein Administrator der MSP den Zugriff auf eine Datei oder ein Programm für den Benutzer eines ferngewarteten Rechners blockieren darf. Auch im Hinblick auf die §§ 6,7 und 8 BDSG erfolgt keine unmittelbare Pflichtverlagerung an den MSP. Die Rechte der Mitarbeiter der ML werden weiterhin gegenüber der ML geltend gemacht.

Vergibt die ML den Auftrag, so ist sie verpflichtet, den MSP dahingehend zu überprüfen, ob dieser den Auftrag überhaupt ordnungsgemäß ausführen kann. Dabei genügt es nicht, eine allgemeine Beurteilung des MSP durchzuführen, da im Gesetzestext die Wortwahl „besondere Berücksichtigung der Eignung“ verwendet wird. Für die Beurteilung der technischen und organisatorischen Maßnahmen ist es notwendig, den MSP auch in dieser Hinsicht auszuwählen. Es ist die dort vorhandene technische Ausstattung zu prüfen, was im Einzelnen die Kontrolle von Zutritt, Zugang, Zugriff, Weitergabe, Eingabe, Auftrag und Verfügbarkeit sowie die Einhaltung des Zweckbindungsgebots betrifft. Vorteilhaft dürften dabei Zertifizierungen des MSP gemäß CobiT, ISO900x, ISO20000 oder ISO2700x sein.

Eine Besonderheit ist zu beachten, wenn der MSP nicht in der EU oder im EWR angesiedelt ist. Dann gilt es für die ML auch, die Anforderungen des § 4b BDSG zu beachten. Insbesondere ist es die Pflicht des ML sicherzustellen, dass ein angemessenes Datenschutzniveau bei dem MSP vorliegt.

Von besonderer Wichtigkeit ist die Anlage zu §9 Satz 1 BDSG. Es ist zwar nicht erforderlich, dass die ML hohe Anforderungen an den MSP stellt; es sind aber zwingende Kriterien des Datenschutzes und der Datensicherheit notwendig, um die technischen und organisatorischen Maßnahmen beurteilen zu können. Für die Grundlegung einer solchen Beurteilung wurde gerade deshalb im vorherigen Kapitel auf die IT-Grundschutz-Kataloge des BSI zurückgegriffen.

Wesentliche Verpflichtungen des MSP sind (§ 11 (4) BDSG): die Verpflichtung der Administratoren der Fernwar-



tung/Fernbetreuung und ggf. weiterer Mitarbeiter auf das Datengeheimnis (§5 BDSG), die Bestellung eines Datenschutzbeauftragten (§ 4f, § 4g BDSG) sowie eine Prüf-, Mitwirkungs- und Mitteilungspflicht.

In der Praxis wird es zwar nicht möglich sein, die Datenverarbeitung des MSP permanent zu überwachen. Andererseits können auch zwischen Überwachungsterminen Fehler auftreten, die bis hin zu Verletzungen des BDSG gehen. Diese hat der MSP der ML aber unverzüglich mitzuteilen. Dabei bezieht sich die Mitteilungspflicht nicht nur auf den Datenbestand der ML, sondern darüber hinaus: Wird der MSP oder werden die bei ihm beschäftigten Personen auffällig gegenüber anderen Kunden, so kann durchaus angenommen werden, dass der MSP nicht in der Lage ist, eine korrekte Fernwartung/Fernbetreuung durchzuführen. Ähnlich wie die neu geschaffene Anzeigepflicht für Datenschutzverletzungen in §42a BDSG hat folglich eine Unterrichtung der ML zu erfolgen. Dieser hat dann die notwendigen Maßnahmen – u.U. auch den Entzug des Auftrags – durchzuführen.

Da die ML verantwortliche Stelle bleibt, sind für das Verfahren der Fernwartung/Fernbetreuung durch die ML noch weitere Vorschriften des BDSG sicherzustellen.

Da ist zunächst die Pflicht zur Datenvermeidung und Datensparsamkeit (§ 3a BDSG).

Eine Anonymisierung oder Pseudonymisierung ist dabei entsprechend dem Einsatzbereich von *Kaseya IT Automation Framework* außerhalb der Berichtserstellung kaum möglich.

Daneben gilt es, so wenig personenbezogene Daten wie möglich für die Fernwartung/Fernbetreuung zu erheben und zu verwenden (§ 3a BDSG).

Hier sind aus Sicht des Autors sechs Fälle besonders kritisch:

1. Über den Agent gelangen automatisch zu viele Daten in den Zugriff des Administrators. Dazu gehört beispielsweise die Erfassung von Inventar, das dem Patch-Management nicht unterliegt. Zu nennen sind hier insbesondere die Erfassung sämtlicher Sekundärspeicher oder die Erfassung sämtlicher Dateien mit der „.exe“-Endung (in der Windows-Welt) und der Anzeige als „Installierte Anwendungen“.

2. Insbesondere bei schlechter Organisation im Hause ML (Stichwort: Vermischung von System- und Benutzerdaten) ist der (versehentliche) Fernzugriff des Administrators auf personenbezogene Daten fast vorprogrammiert. Sollte ein Mitarbeiter der ML beispielsweise seine privaten Zugangsdaten zu seinen Privatkonten unverschlüsselt in einer Datei „password.dat“ ablegen, so werden Zugriffe fast herausgefordert[28]. Zudem mögen auf den ferngewarteten Rechnern personenbezogene Daten von Kunden, Lieferanten, … der ML abgelegt sein, für die die ML eine Schutzverpflichtung hat.

3. Es ist für die Zwecke der Fernwartung/Fernbetreuung oft unerheblich, „Wann-Wer-Wie lange-Was“ an einem ferngewarteten Rechner getan hat. Lediglich das „Wann-Was“ ist im Fehlerfall von Bedeutung. Die Erfassung der zusätzlichen Informationen erleichtert zwar die Arbeiten und gestattet Reaktionen (Sanktionen), ist aber nicht zwingend erforderlich. So ist nicht verständlich, warum beispielsweise ein Eintreten in einen Energiesparmodus eines ferngewarteten Rechners mit der Information erfasst werden muss, welcher Benutzer dies veranlasste.

4. Die vielfältigen Möglichkeiten der automatisierten Ereignisüberwachung auf den ferngewarteten Rechnern. Es ist beispielsweise nicht unmittelbar einsichtig, warum für die Fernwartung eine umge-

[28] Dies bietet auch Ansatzpunkte für eine Prüfung des MSP. Das Stichwort dazu heißt **Honeypots**: Dabei werden Köder in den ferngewarteten Rechnern ausgelegt und es werden alle Zugriffe auf die Köder sorgfältig protokolliert und analysiert.

hende Benachrichtigung des Administrators erfolgen sollte, wenn ein Programm installiert wurde. Diese Recherche kann auch später bei einer für den Benutzer transparenten Wartung des Systems in den Protokolldateien erfolgen.

5. Die weitgehend unbegrenzten Möglichkeiten der Berichtserstellung. Hier ist schwer zu vermeiden, dass unzulässige Verwendungen erfolgen, denn schließlich kann man beispielsweise in einer Einwilligung nicht auf alle Möglichkeiten hinweisen.

6. Schließlich kommt hinzu, dass potenziell ein direkter Zugriff auf die Datenbank mit Exportmöglichkeiten möglich ist. Dies erlaubt dann beispielsweise die Erstellung von vergleichenden Nutzungsprofilen: Im Webportal erhalte ich über **System-Benutzersicherheit-Benutzerhistorie** eine Liste der Funktionen mit Datums- und Zeitangabe, auf die ein Administrator zugegriffen hat. Extrahiere ich nun diese Daten gar aus der Tabelle **dbo.adminHistory** der Datenbank ***ksubscribers*** für alle Administratoren, so kann ich vergleichende Nutzungsprofile erstellen, die dann etwa für eine Leistungsbewertung missbraucht werden können.

Dann ist vor allem die Frage der Zulässigkeit zu klären. Genau genommen geht es um zwei Zulässigkeiten: Die Zulässigkeit der Erhebung und Verwendung von personenbezogenen Daten über die Nutzer ferngewarteter Rechner durch den Kaseya Agent (inklusive flankierender Software) und die Zulässigkeit der Erhebung und Verwendung personenbezogener Daten über die Nutzer des Kaseya Webportals.

§ 4 BDSG bejaht die Zulässigkeit nur, „soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat".

Hier ist sicherlich im konkreten Anwendungsfall eine Vorabkontrolle durch einen Datenschutzbeauftragten und/oder die Beratung durch einen Fachanwalt erforderlich, letzteres insbesondere wenn auch andere Rechtsvorschriften als das BDSG zur Anwendung kommen können.

Aus der Sicht des Autors greifen jedoch die Erlaubnistatbestände des BDSG (hier insbesondere § 28 (1) BDSG) für die ML typisch nicht, da zunächst die spezifische Datenerhebung und Datenverwendung für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit den Mitarbeitern im Hause ML typisch nicht erforderlich ist. Zudem hat die ML zwar ein berechtigtes Interesse an der Wartung ihrer Rechner und der Betreuung ihrer Mitarbeiter. Für die Wahrung dieses Interesses ist aber der Einsatz des *Kaseya IT Automation Framework* ebenfalls nicht erforderlich. Schließlich gibt es auch – wie geschildert – gute Gründe dafür, dass das schutzwürdige Interesse der Mitarbeiter der ML an dem Ausschluss der Verarbeitung oder Nutzung gegenüber dem berechtigten Interesse der ML überwiegt.

Anders liegt aus der Sicht des Autors der Fall beim MSP. Hier wird das *Kaseya IT Automation Framework* über das Webportal zur Steuerung von internen Geschäftsprozessen verwendet und ist somit für die Durchführung des Beschäftigungsverhältnisses der betroffenen Mitarbeiter im Hause MSP erforderlich. Die erfassten personenbezogenen Daten der Mitarbeiter der MSP sind zudem erforderlich, um beispielsweise Revisionssicherheit herzustellen. § 28 (1) BDSG kann folglich hier die Zulässigkeit begründen. Es ist aber zu beachten, dass auch dann die Zwecke der Erhebung und Verwendung konkret festzulegen sind.

Diese letztgenannte Argumentation greift jedoch nicht für Mitarbeiter der ML, die ggf. auch über das Webportal das *Kaseya IT Automation Framework* nutzen.

In summa bleibt festzuhalten, dass aus Sicht des Autors für die Mitarbeiter der ML wohl Einwilligungen hinsichtlich des Einsatzes von Kaseya Agent (inklusive flankierender Software) und hinsichtlich der Webportalnutzung erforderlich sind, während für die Mitarbeiter der MSP auf eine Einwilligung hinsichtlich der Webportalnutzung verzichtet werden kann.



Da die Geschäftsprozesse der Fernwartung/Fernbetreuung jedoch extrem davon profitieren, dass sowohl Vertrauen zu den eingesetzten Werkzeugen als auch zu und zwischen den beteiligten Personen und Institutionen besteht, empfiehlt der Autor jedoch generell den Einsatz von Einwilligungen. Dies auch aus Gründen der Transparenz (siehe unten).

Dabei bedarf es jeweils einer "informierten Einwilligung“: Betroffene können grundsätzlich nur in diejenigen Umstände rechtswirksam einwilligen, von denen sie sich eine hinreichend bestimmte Vorstellung machen können. Demgemäß ist bei der Einholung der Einwilligung etwa bei Mitarbeitern der ML zum Kaseya Agent auf die Bedeutung der Einwilligung („Aufrechterhaltung des IT-Betriebs“), den Zweck der Erhebung und Verwendung („Fernwartung/Fernbetreuung“) sowie auf das Recht und die Folgen der Verweigerung der Einwilligung hinzuweisen. Neben der Schriftform kommen ggf. elektronische Einwilligungen in Frage. In den Anhängen B und C sind Beispiele für die möglichen Inhalte derartiger Einwilligungen angegeben.

Weiterhin ist das Gebot der Transparenz zu beachten, insbesondere die Pflicht zur Unterrichtung der Nutzer bezüglich der Erhebung und Verwendung (siehe § 4 BDSG). Eine in der Praxis geläufige Form der Unterrichtung ist eine Datenschutzerklärung, die über Hintergründe, Umfänge, Zwecke und Konsequenzen der Erhebungen und Verwendungen Auskunft gibt. Im Falle des *Kaseya IT Automation Framework* sind dazu ggf. zwei Erklärungen notwendig: Eine für die Benutzer des Webportals und eine weitere für die Personen, die einen ferngewarteten Rechner nutzen. Erstere könnte in das Webportal eingebunden werden, letztere in den Kaseya Agent. Die Anhänge D und E geben beispielhaft wünschenswerte Inhalte wieder.

Für den Betrieb des *Kaseya IT Automation Framework* ist schließlich von der ML als verantwortlicher Stelle eine Verfahrensbeschreibung mit den gesetzlich vorgegebenen Inhalten zu erstellen und ggf. zu melden (§ 4d, 4e BDSG). Die vorgeschriebenen Inhalte sind in der Regel verhältnismäßig unproblematisch. Im Anhang A ist ein Beispiel angegeben.

IMPLIKATIONEN DES TMG

Durch den Betrieb des Kaseya Webportals wird der MSP zum Diensteanbieter im Sinne des TMG (siehe Seite 13). Damit unterliegt der MSP – nach Ansicht des Autors - der Impressumspflicht nach § 5 TMG. Zwar heißt es im Gesetzestext: "Diensteanbieter haben für geschäftsmäßige, in der Regel gegen Entgelt angebotene Telemedien folgende Informationen leicht erkennbar, unmittelbar erreichbar und ständig verfügbar zu halten." Rein dem Wortlaut nach unterlägen somit alle Webseiten von kommerziellen Anbietern keiner Impressumspflicht, wenn sie keine kostenpflichtigen Dienste für die Nutzer (hier vorrangig die Administratoren aus dem Hause MSP) anbieten würden. Eine solche Interpretation ist in Juristenkreisen jedoch strittig und auch mit der Entstehungsgeschichte des TMG nicht vereinbar. Insofern sollte - nach Ansicht des Autors - die Vorschrift entsprechend ihrem Sinn und Zweck ausgelegt werden: Webseiten mit geschäftlichem Hintergrund, egal ob sie kostenpflichtige Inhalte anbieten oder nicht, sollten eine Anbieterkennzeichnung gemäß § 5 TMG haben.

Dabei ist zu beachten, dass diese leicht erkennbar, unmittelbar erreichbar und ständig verfügbar ist. Der BGH hat dazu in 2006 entschieden, dass eine Anbieterkennzeichnung auch dann noch „unmittelbar erreichbar“ sei, wenn sie nicht direkt auf der Hauptseite stehe, sondern erst durch zwei Links erreichbar sei.

Problematisch ist in diesem Zusammenhang, dass die Konfiguration des Webportals bislang gar keine Möglichkeit vorsieht, eine Anbieterkennzeichnung adäquat einzubinden und verfügbar zu machen.

Der Abschnitt 4 des TMG mit Regelungen zum Datenschutz ist - nach Einschätzung des Autors - beim Einsatz des *Kaseya IT Automation Framework* nicht anwendbar, da § 11 (1) TMG die Geltung verneint, wenn „die Bereitstellung solcher Dienste

1. im Dienst- und Arbeitsverhältnis zu ausschließlich beruflichen oder dienstlichen Zwecken oder

2. innerhalb von oder zwischen nicht öffentlichen Stellen oder öffentlichen Stellen ausschließlich zur Steuerung von Arbeits- oder Geschäftsprozessen erfolgt“.

Eine andere rechtliche Bewertung hinsichtlich der Datenschutzregelung im TMG hätte beim Einsatz des *Kaseya IT Automation Framework* im Übrigen hauptsächlich zur Folge, dass eine Datenschutzerklärung (mehr oder weniger) verpflichtend wäre und dass hinsichtlich der Erhebung und Verwendung von Bestands- und Nutzungsdaten strenge Regeln verpflichtend anzuwenden wären. Aus Sicht des Autors folgen diese Verpflichtungen beim *Einsatz des Kaseya IT Automation Framework* jedoch bereits aus den im BDSG verlangten Prinzipien der Transparenz und der Datensparsamkeit.

IMPLIKATIONEN DES TKG

Ebenso nicht generell anwendbar sind - nach Einschätzung des Autors - die Regelungen zum Datenschutz in Abschnitt 2 des TKG, da allein durch den Einsatz des *Kaseya IT Automation Framework* nicht geschäftsmäßig Telekommunikationsdienste erbracht werden.

Eine andere rechtliche Bewertung hinsichtlich der Datenschutzregelungen im TKG hätte beim Einsatz des *Kaseya IT Automation Framework* im Übrigen hauptsächlich zur Folge, dass bezüglich der Verwendung von Verkehrsdaten strenge Regeln verpflichtend anzuwenden wären. Aus Sicht des Autors folgt diese Verpflichtung beim Einsatz des *Kaseya IT Automation Framework* jedoch bereits aus dem im BDSG verlangten Prinzip der Erforderlichkeit.

IMPLIKATIONEN DES STGB

Auch das Strafgesetzbuch (StGB) enthält – zumindest indirekt – Vorschriften zum Datenschutz. Hier sind insbesondere die §§ 202a und 202b über das Ausspähen und Abfangen von Daten zu nennen.

Dabei gilt es zu beachten, dass ein Mitarbeiter der MSP schon dann „unbefugt“ handelt, wenn er Daten der Fernwartung außerhalb des Vertragsrahmens verwendet.



RICHTLINIEN FÜR DEN DATENSCHUTZKONFORMEN EINSATZ DER VERSION MSE K2

Bei den nachfolgenden Empfehlungen zu technischen und organisatorischen Maßnahmen ist je nach konkreter Sachlage selbstverständlich noch zu prüfen, ob der Aufwand für die Maßnahmen verhältnismäßig ist. Schließlich verlangt der Gesetzgeber keinen unverhältnismäßigen Aufwand in Sachen Datenschutz!

TECHNISCHE MASSNAHMEN ZUR SICHERUNG DES DATENSCHUTZKONFORMEN BETRIEBS

EMPFEHLUNGEN ZUR ZUTRITTSKONTROLLE

Für die Zutrittskontrolle in das Gebäude und die Gebäudebereiche des MSP ist es empfehlenswert, dass Schlüsselregelungen existieren oder Berechtigungsausweise, die durch einen Pförtner kontrolliert werden.

Es wird empfohlen, dass alle Besucher des Gebäudes eindeutig Mitarbeitern des MSP zugeordnet werden, die für sie während ihres Aufenthaltes verantwortlich sind und sie durchgehend beaufsichtigen.

Bei Serverräumen wird empfohlen, dass jeder Zutritt protokolliert wird und ggf. durch höherwertige Zutrittskontrollmechanismen (Biometrie, RFID, …) geschützt wird. Eine Kennzeichnung der Serverräume sollte nicht erfolgen.

Bei Beachtung dieser Empfehlungen ist im Bereich Zutrittskontrolle die Datenschutzkonformität **vorbildlich**.

EMPFEHLUNGEN ZUR ZUGANGSKONTROLLE

Ein erster Schritt in Richtung empfohlener Zugangskontrolle erfordert den Betrieb des Kaseya Server und des Kaseya Webportals auf dedizierter Hardware (siehe dazu Seite 36)[29].

Die unbefugte Nutzung des Kaseya Webportals selbst wird durch ein einstellbares Anmeldeverfahren auf Basis von Benutzerkennungen und Benutzerkennworten verhindert. Benutzerkennworte und übermittelte Anmeldedaten sind dabei gegen Offenlegung ausreichend sicher geschützt (siehe Seite 33). Eine Vorschlagsfunktion für sichere Benutzerkennworte ist ebenfalls integriert.

Die Einstellmöglichkeiten einschließlich der empfohlenen Einstellungen sind wie folgt (vergleiche dazu auch Seite 71):

- Anzahl N der erfolglosen Anmeldeversuche in Folge, bevor der Zugang für eine Benutzerkennung für die Zeitdauer M gesperrt wird (N = 5; M = 1 Stunde)
- Minuten S der Inaktivität, bevor eine Anmeldung beendet wird (S = 10)
- Verhindern, dass Personen ihre Benutzerkennung ändern (Ja)
- Erfordert Benutzerkennwortänderung alle N Tage (N=30)
- Mindestlänge M des Benutzerkennworts durchsetzen (M=8)
- Benutzerkennwortwiederholung verbieten für K Generationen (K=3)
- Groß- und Kleinbuchstaben im Benutzerkennwort erforderlich (Ja)
- Sowohl Buchstaben als auch Zahlen im Benutzerkennwort erforderlich (Ja)
- Sonderzeichen im Benutzerkennwort erforderlich (Ja)

[29] Ein weiterer Grund hierfür ist, dass der Hersteller seinen Server Support an diese Vorgabe koppelt.

Ein Anmeldeversuch kann auch daran scheitern, dass für die gewählte Rolle des befugten Benutzers Einschränkungen der Anmeldezeiten vorgegeben sind. Diese können je Wochentag individuell für jede Rolle festgelegt werden.

Die Benutzerkennung-/Benutzerkennwortnutzung inklusive Anmeldezeiten wird protokolliert und das Protokoll sollte – so die Empfehlung - 30 Tage aufbewahrt werden.

Bei Beachtung dieser empfohlenen Einstellungen und durch eine angemessene Festlegung von Anmeldestunden ist im Bereich Zugangskontrolle die Datenschutzkonformität **sehr hoch**[30].

EMPFEHLUNGEN ZUR ZUGRIFFSKONTROLLE

Unabdingbar für eine wirksame Zugriffskontrolle ist zunächst, dass die Mitarbeiter des MSP nie unter einer Sammelbenutzerkennung arbeiten. Dies ist auch Voraussetzung für eine revisionssichere Protokollierung aller Zugriffe.

Das Kaseya IT Automation Framework verwendet zur Steuerung der Zugriffskontrolle **Rollenmodelle in Verbindung mit Umfangdefinitionen** zur Konfiguration und Administration der Zugriffskontrolle eines befugten Benutzers. Für eine **Rolle (role)**, wie Administrator (typisch aus dem Hause MSP), Endbenutzer (typisch aus dem Hause ML) oder Service-Desk-Mitarbeiter, kann und muss definiert werden, welche Funktionen im Kaseya Webportal und über Kaseya Live Connect (KLC) wann zur Verfügung stehen. Zusätzlich zu (mindestens) einer Rolle wird jedem befugten Nutzer dann noch (mindestens) ein **Umfang (scope)** zugeordnet. Dieser Umfang definiert genauestens welche ferngewarteten Rechner im Zugriff dieses befugten Nutzers liegen. Dabei können die Rechner, die im Zugriff liegen sollen, auch auf den Ebenen Organisation, Abteilung und Rechnergruppen bestimmt werden. Im Extremfall können also befugte Benutzer nur Zugriff auf eine einzige Funktion für einen einzigen ferngewarteten Rechner haben. Damit ist jede Zugriffskontrolle zunächst begrenzt bis hinunter zur Rechnerebene und dann – über die Funktionsbeschränkung – sogar bis zur Datenebene realisierbar. Dabei ist aber zu beachten, dass jedem befugten Nutzer mehrere Rollen und/oder Umfänge zugeordnet werden können. Allerdings können zu einer bestimmten Zeit nur eine Rolle und ein Umfang aktiv sein.

Bei einer Vergabe von personengebundenen Benutzerkennungen und bei guter Planung und Administration der vorhandenen Möglichkeiten der Zugriffskontrolle unter Berücksichtigung der Beteiligten und ihrer Umstände ist die Datenschutzkonformität im Bereich Zugriffskontrolle also **weitgehend vorbildlich** gestaltbar[31].

---

[30] Dies bedeutet NICHT, dass die Möglichkeiten der IT-Sicherheit hinsichtlich Zugangskontrolle durch die genannten Empfehlungen ausgeschöpft sind. Da Windows-Betriebssysteme beim Einsatz von IIS in der Vergangenheit häufiger dadurch auffielen, dass Schwachstellen entdeckt wurden, ist es nach Ansicht des Autors sogar empfehlenswert, die Zugangskontrolle durch ein dem Server des Kaseya Webportals hardwaremäßig vorgeschaltetes Authentifizierungssystem (etwa auf einem Proxy-Server) zusätzlich abzusichern. Allein der Datenschutz kann eine solche Maßnahme allerdings nicht rechtfertigen, so dass dies nicht Bestandteil der hier formulierten Empfehlungen ist.

[31] Dabei ist zu beachten, dass die Funktionsbeschränkung auf Basis der Deaktivierung von Menüeinträgen erfolgt. Leider (Stichwort: Usability) sind manche Funktionen über mehrere Menüeinträge abrufbar (siehe etwa „Dokumente“). Um eine wirksame Funktionsbeschränkung zu konfigurieren, müssen daher alle entsprechenden Menüeinträge deaktiviert werden. Hier ist also große Sorgfalt geboten.



EMPFEHLUNGEN ZUR WEITERGABEKONTROLLE

Es wird empfohlen, dass der MSP bei der Erstellung, dem Transport, der Lagerung und der Vernichtung von Datenträgern die heute übliche Sorgfalt walten lässt. Als Minimum ist hier eine Dienst- bzw. Betriebsvereinbarung nötig, die insbesondere die Erstellung und Sicherung mobiler Datenträger regelt. Hier gilt es zu beachten, dass Verschlüsselung auch hilft, „ruhende“ Daten zu schützen. Obwohl man mehrere Vorsichtsmaßnahmen ergreifen kann, um eine Datenbank zu schützen, indem man beispielsweise die Datenbankserver mit einer Firewall umgibt, stellen die physischen Datenträger, auf denen die Datenbank gespeichert ist (auch die Sicherungskopien), eine ganz andere Art von Sicherheitsrisiko dar. Eine böswillige Person könnte diese stehlen und unter Umständen auf die gespeicherten Daten zugreifen, wenn die Verschlüsselung fehlt.

Die Datenübertragungen zwischen Kaseya Agent und Kaseya Server sind wirksam verschlüsselt und können als ausreichend sicher gelten.

Hinsichtlich Fernzugriff, Dateiübertragung und Chat ist eine Verschlüsselung möglich und diese sollte auch eingesetzt werden. Empfohlen wird die Verwendung des Advanced Encryption Standard (AES).

Für den Datentransport zwischen dem Kaseya Webportal und einem Browser wird die verpflichtende Nutzung des HTTPS-Protokolls empfohlen.

Außerdem ist es empfehlenswert, sämtlichen Email-Verkehr, der bei der Durchführung der Fernwartung/Fernbetreuung entsteht, wirksam gegen unbefugte Einsichtnahme zu schützen. Möglich ist hier der Einsatz von SSL oder PGP oder ähnlichen Ansätzen.

Entsprechend den fast selbstverständlichen Regelungen für Papierkörbe wird empfohlen, bei den für den Zugang zum Webportal verwendeten Browsern die Historie unmittelbar nach einer Abmeldung vom Webportal zu löschen.

Bei Beachtung dieser Empfehlungen ist im Bereich Weitergabekontrolle die Datenschutzkonformität **sehr hoch**[32].

EMPFEHLUNGEN ZUR EINGABEKONTROLLE

Die umfangreiche Sammlung von Log-Daten und Protokolldaten (siehe Seite 48 f) gestattet im Nachhinein die Ermittlung, wer Daten zu welcher Zeit eingegeben oder verändert hat[33]. Eine generelle Empfehlung für die Dauer der Speicherung von Log-Daten und Protokolldaten ist nicht möglich. Als Faustregel sollte aber eine Spanne bis zu 1 Monat ins Auge gefasst werden. Archivierungen von Log-Daten und Protokolldaten sind aus Gründen der Datensparsamkeit nur im Zuge von Systemsicherungen zuzulassen.

Im Bereich Eingabekontrolle ist die Datenschutzkonformität also bei Beachtung der genannten Empfehlungen **vorbildlich**.

---

[32] Eine bessere Bewertung scheint nicht angezeigt, da die Datenschutzkonformität in Teilen abhängig vom „richtigen“ Verhalten der Mitarbeiter ist.

[33] Dies erfordert natürlich – wie bereits bei der Zugriffskontrolle erörtert – eine personengebundene Vergabe von Benutzerkennungen.



EMPFEHLUNGEN ZUR AUFTRAGSKONTROLLE

Die Auftragskontrolle ist durch die Form- und Inhaltsvorschriften des § 11 BDSG für die Fernwartung ausreichend geregelt. Beim Einsatz der optionalen Module für die Fernbetreuung sind entsprechende Klauseln in den Auftrag aufzunehmen.

Eine vorbildliche Bewertung der Datenschutzkonformität kann jedoch im Bereich Auftragskontrolle nicht erfolgen, da im Betrieb auf Vertragspflichten zurückgegriffen werden muss[34]. So ist es beispielsweise unter Umständen denkbar, dass bei einem Verstoß gegen die Überwachungspflichten durch den Kunden der Fernwartung/Fernbetreuung und einem gleichzeitig vorliegenden pflichtwidrigen Verhalten der fernwartenden Administratoren ein unzulässiger Zugriff auf personenbezogene Daten erfolgen kann.

Somit ist also im Bereich Auftragskontrolle die Datenschutzkonformität nur **sehr hoch**.

EMPFEHLUNGEN ZUR VERFÜGBARKEITSKONTROLLE

Es wird empfohlen, das Betriebsgebäude des MSP mit einer Blitzschutzanlage und einer Brandschutzanlage auszustatten. Die Elektroinstallation sollte mindestens den tatsächlichen Anschlusswerten entsprechen. Eine Gefahrenmeldeanlage für Einbruch, Brand und Wasser sollte vorhanden sein und eine Weiterleitung der Meldungen an eine ständig besetzte Stelle (Pförtner, Wach- und Sicherheitsdienst, Feuerwehr, etc.) sollte rund um die Uhr erfolgen.

Die Hardware, auf dem der Kaseya Server und das Kaseya Webportal betrieben werden (MSP-S-1 in der Referenzinstallation), sollte in einem Serverraum des Betriebsgebäudes des MSP installiert werden. Dieser Raum sollte mit feuerhemmenden und rauchdichten Sicherheitstüren und –fenstern ausgestattet sein.

Je nach Anzahl der ferngewarteten Rechner sollte die Hardware und Software für den Kaseya Server und das Kaseya Webportal beim MSP deutlich besser als in der minimalen Anforderung gefordert ausgelegt werden. Der Hersteller empfiehlt etwa bei bis zu 2500 ferngewarteten Maschinen folgende Ausstattung:

- Dual Processor (Intel Xeon 3 GHz Quad Core, 1066 MHz FSB,4 MB Cache)
- 10 GB RAM
- Datenbank RAID: 3x73Gig 10k SAS (Hardware RAID 5)
- Betriebssystem RAID: 2x73Gig 10k SAS (Hardware RAID 1)
- Microsoft Windows Server 2003 or 2008 Standard Edition 64 Bit
- Microsoft SQL Server 2005 or 2008 Standard Edition 64 Bit
- Ethernet: 1 Gbps
- Internet: T1

Eine bessere Verfügbarkeit kann auch dadurch erzielt werden, dass der Kaseya Server und das Kaseya Webportal auf separater, dedizierter Hardware betrieben werden. Möglich ist auch ein redundanter Betrieb mit primären und sekundären Systemen.

Sicherungskopien der Datenbestände des Kaseya Server und des Kaseya Webportals sollten außerhalb des Betriebsgebäudes des MSP sicher aufbewahrt werden.

---

[34] Eine Notwendigkeit, die nicht produktspezifisch ist und die wohl nahezu bei allen automatisierten Verfahren der Fernwartung/Fernbetreuung vorliegt.

Bei Beachtung dieser Empfehlungen ist im Bereich Verfügbarkeitskontrolle die Datenschutzkonformität also **vorbildlich**.

EMPFEHLUNGEN ZUR ZWECKBINDUNGSKONTROLLE

Zunächst ist auch aus Gründen der Zweckbindungskontrolle dringend zu empfehlen, den Zugriff auf die Systemdatenbank außerhalb des Webportals (**System-Datenbankzugriff-Datenbankansichten**) effektiv zu sperren.

Wie bereits bei der Zugriffskontrolle erwähnt, gestatten die Festlegung und Zuordnung von Rollen und Umfängen eine effektive und effiziente Trennung der Daten innerhalb des Webportals.

Ein Administrator hat so (im Regelfall) nur die Daten einer ML im Zugriff. Ist er für mehrere Kunden verantwortlich, muss er seine Rolle und/oder seinen Umfang neu wählen.

Eine physikalische Trennung der Daten (getrennte Tabellen, separate Datenbanken, …) ist derzeit nicht möglich.

Bei guter Planung und Administration ist also die Datenschutzkonformität im Bereich Zweckbindungskontrolle **weitgehend vorbildlich**.

ORGANISATORISCHE MASSNAHMEN ZUR SICHERSTELLUNG DES DATENSCHUTZKONFORMEN BETRIEBS

EMPFEHLUNGEN FÜR DEN MSP

BESTELLUNG EINES DATENSCHUTZBEAUFTRAGTEN

Wie bereits ausgeführt (siehe Seite 74 f), hat der MSP einen Datenschutzbeauftragten zu bestellen. Dabei ist besonders darauf zu achten, dass der Kandidat ausreichende Fachkunde in der Fernwartung/Fernbetreuung allgemein und zu *Kaseya IT Automation Framework* speziell besitzt.

Vor Einsatz, Erweiterung oder erheblicher Veränderung des *Kaseya IT Automation Framework* hat der MSP diesen Datenschutzbeauftragten zu involvieren. Zur Beurteilung der datenschutzrechtlichen Zulässigkeit eines Verfahrens der Fernwartung/Fernbetreuung sind ihm vom MSP alle relevanten Unterlagen zur Verfügung zu stellen.

ERSTELLUNG VON SICHERHEITSRICHTLINIEN

Es wird empfohlen, sowohl eine „**PC-Richtlinie**" als auch eine „**Sicherheitsrichtlinie zum Einsatz von *Kaseya IT Automation Framework***" zu erstellen. Die erforderlichen Inhalte entsprechend IT-Grundschutz sind auf den Seiten 63 f beschrieben.

EINHOLUNG VON EINWILLIGUNGEN FÜR DIE NUTZUNG DES WEBPORTALS

Über jeden befugten Benutzer des Kaseya Webportals werden personenbezogene Daten automatisch in einer Historie der Nutzung des Webportals und einer Historie der Konfigurationsänderungen erhoben und verarbeitet (siehe Seite 61). Hierfür ist eine Einwilligung empfehlenswert (siehe Seite 74 f). Ein Beispiel dazu findet sich in Anhang C.

ARBEITSANWEISUNGEN ZUR NUTZUNG DES WEBPORTALS

Zur Sicherstellung der Vertragserfüllung wird empfohlen, dass mit der Bekanntgabe der Zugangsdaten (Benutzerkennung, Benutzerkennwort) auch Hinweise zur Nutzung des Webportals bekannt gegeben werden. Hier sind die vertraglichen Besonderheiten der spezifischen Fernwartung/Fernbetreuung detailliert aufzuführen.

Insbesondere sind Bedingungen, Vorgehensweisen und Details zur Ausführung von Fernzugriffen festzulegen und zu dokumentieren. Für eine gewisse Softwarewartung können solche Anweisungen zum Fernzugriff etwa wie folgt aussehen:

> Behebung von Fehlerzuständen in der Anwendung XYZ in der Abteilung N.
> Gestattet sind folgende Zugriffe:
>> Schreibender Zugriff auf die Konfigurationsdatei ....
>> Lesender Zugriff auf die anderen Dateien im Programmverzeichnis ....

Hinzu kommen Vorgaben für die Installation und Konfiguration der Agenten und der weiteren Software auf den ferngewarteten Rechnern.

Daneben sollte auf datenschutzrechtlich „korrektes“ Verhalten hingewiesen werden. Hier ist insbesondere erforderlich, bei Auswertungen auf das Anonymisierungsgebot zu drängen. Auch Dateiübertragungen und Dateieinsichten sollten mit Blick auf den Datenschutz thematisiert werden.

DATENSCHUTZERKLÄRUNG IM WEBPORTAL

Da auch personenbezogene Daten der Nutzer des Webportals erhoben und verwendet werden, ist eine Datenschutzerklärung empfehlenswert (siehe Seite 77 f). Diese sollte in das Webportal integriert werden. Insbesondere ist in dieser Erklärung auf die automatische Speicherung von Funktionsaufrufen mit Zeitstempel und deren Konsequenzen sowie auf eine mögliche Auswertung hinzuweisen. Ein Beispiel findet sich in Anhang D.

EMPFEHLUNGEN FÜR DIE ML

AUSGESTALTUNG DER AUFTRAGSDATENVERARBEITUNG

Das BDSG verlangt von der ML eine präzise Festlegung der zulässigen Wartungs- und Betreuungstätigkeiten. Insbesondere sind (entsprechend den weiter oben aufgeführten Empfehlungen) u.a. folgende Fragen zu beantworten:

1. Welche Auswertungen der Daten sind gestattet?
2. Welcher Administrator hat welchen Zugriff auf die Daten?
3. Wie sind die diversen Softwarepakete (Agent, VNC, …) auf dem ferngewarteten Rechner zu installieren und zu konfigurieren?
4. Darf ein Fernzugriff auf den ferngewarteten Rechner ohne Kenntnis oder Zustimmung des jeweiligen Benutzers geschehen?
5. Wann und wie ist eine Veränderung oder Blockierung der Dateien und Programme auf dem ferngewarteten Rechner zulässig?



6. Welche Protokolle müssen in welchem Detail erstellt werden?

7. Wann sind welche Daten zu löschen?

Beispielhafte Festlegungen zu diesen Punkten könnten etwa wie folgt formuliert werden:

Zu 1.:
Ein Administrator der Fernwartung darf Daten nur in dem für die Durchführung der Fernwartung unerlässlich notwendigen Umfang erheben und verwenden.

Zu 2.:
Administratoren der Fernwartung dürfen nur solche Mitarbeiter sein, die entsprechend § 5 BDSG auf das Datengeheimnis schriftlich verpflichtet worden sind und die für die Fernwartung auf Basis des *Kaseya IT Automation Framework* besonders geeignet sind.

Administratoren, die Fernwartung für Dritte durchführen, dürfen während dieser Tätigkeiten keinen Zugriff auf Daten dieser Fernwartung herstellen können.

Zu 3.:
Die Installation und der Betrieb von Software, die für die Fernwartung auf einem Rechner benötigt wird, müssen voll umfänglich transparent für die Person sein, die den ferngewarteten Rechner benutzt.

Zu 4.:
Der Fernzugriff auf einen ferngewarteten Rechner ist nur in begründeten Ausnahmefällen zulässig. Der Aufbau der Verbindung muss durch die Person gestattet werden, die den ferngewarteten Rechner benutzt oder benutzen darf. Eine Ausnahme von dieser Regel ist nicht vorgesehen. Die entsprechenden Vorgänge sind zu protokollieren.

Zu 5.:
Ein Administrator der Fernwartung darf Dateien und Programme auf dem ferngewarteten Rechner nur dann ändern oder blockieren, wenn er dafür zuvor die Erlaubnis der Person eingeholt hat, die den ferngewarteten Rechner benutzt. In begründeten Ausnahmefällen kann diese Erlaubnis nachträglich eingeholt werden. Die entsprechenden Vorgänge sind zu protokollieren.

Zu 6.:
Sämtliche Funktionen, auf die ein Administrator der Fernwartung zugreift, und eventuelle Änderungen von Daten sind mit Zeitstempel inhaltlich zu protokollieren. Die Protokolle sind mindestens 20 Tage aufzubewahren.

Zu 7.:
Zu vernichtende Unterlagen werden ordnungsgemäß entsorgt, ohne dass unbefugte Personen von den Daten Kenntnis erlangen können (z.B. durch ein geeignetes Entsorgungsfachunternehmen).

Nach Beendigung der Geschäftsbeziehungen werden alle Unterlagen zurückgegeben oder gelöscht, soweit nicht berechtigte Gründe (etwa im Sinne von § 35 (3) BDSG) entgegenstehen.

ERSTELLUNG EINER VERFAHRENSBESCHREIBUNG

Vor dem tatsächlichen Einsatz des *Kaseya IT Automation Framework* muss die ML eine Verfahrensbeschreibung gemäß § 5e BDSG erstellen. Ein Beispiel für eine derartige Verfahrensbeschreibung findet sich in Anhang A.

INDIVIDUELLE EINWILLIGUNGEN ZUM EINSATZ DES KASEYA IT AUTOMATION FRAMEWORK

Über jeden befugten Benutzer eines ferngewarteten Rechners werden personenbezogene Daten erhoben und verwendet (siehe Seite 57 f). Hierfür ist eine Einwilligung empfehlenswert (siehe Seite 74 f). Ein Beispiel dazu

findet sich in Anhang B.

DIENST- ODER BETRIEBSVEREINBARUNG ZUM EINSATZ DES KASEYA IT AUTOMATION FRAMEWORK

Wie bei jedem automatisierten Verfahren ist es empfehlenswert, die Rahmenbedingungen für den Einsatz des *Kaseya IT Automation Framework* festzuschreiben. Hierfür bietet sich eine Dienst- oder Betriebsvereinbarung an. Sie sollte beispielhaft inhaltlich folgende Punkte umfassen:

1. Personenbezogene Daten werden beim Einsatz des Verfahrens nur zu dem Zweck der Fernwartung/Fernbetreuung erhoben und verwendet.
2. Das Verfahren dient grundsätzlich nicht der Leistungs- und Verhaltenskontrolle im Sinne des § 87 Abs. 1 Nr. 6 BetrVG. Erlangte Informationen über die Arbeitsweise und das Verhalten von Arbeitnehmern werden nicht zum Nachteil der betroffenen Arbeitnehmer verwendet.
3. Soweit erforderlich, wird der einzelne Arbeitnehmer auf Kosten des Arbeitgebers in der Nutzung des Verfahrens geschult.
4. Jeder Arbeitnehmer hat das Recht, jederzeit Einsicht in die über ihn gespeicherten Daten zu nehmen.
5. Die Nutzung von verdeckten Verbindungen zur Datenübertragung ist untersagt.

Wie bereits erwähnt, muss die ML auch sicherstellen, dass der MSP personenbezogene Daten nur soweit zur Kenntnis nehmen kann, wie dies unvermeidlich ist. Daher empfiehlt sich – falls nicht anderweitig schon geregelt - eine Ergänzung dieser Dienst- oder Betriebsvereinbarung, die jedem Mitarbeiter inhaltlich zumindest folgende Verpflichtungen auferlegt:

6. Personenbezogene Daten auf den ferngewarteten Rechnern sind gegen unbefugte Zugriffe und Missbrauch zu schützen. Eine Speicherung personenbezogener Daten durch den Arbeitnehmer ist daher nur in verschlüsselten Bereichen zulässig und der Arbeitnehmer hat dafür Sorge zu tragen, dass seine Schlüssel keinem Außenstehenden und auch keinem anderen Mitarbeiter bekannt werden.
7. Das Speichern personenbezogener Daten ist nur auf den dafür vorgesehenen und entsprechend gesicherten Datenträgern gestattet.
8. Das Speichern personenbezogener Daten auf Wechseldatenträgern ist ausdrücklich verboten.

EMPFEHLUNGEN FÜR DEN HERSTELLER

PRODUKTWEITERENTWICKLUNG

Die Verschlüsselung der Datenbestände im *Kaseya IT Automation Framework* wäre eine konsequente Fortführung der Philosophie, die sich etwa bereits bei der sicheren Agent-Server-Kommunikation zeigt. Dabei sollte beachtet werden, dass Daten nicht nur in der Datenbank sondern auch in anderen Dateien abgelegt werden. Bei der Datenbank empfiehlt sich möglicherweise zunächst der Einsatz der transparenten Datenverschlüsselung (siehe Seite 34 f), da hier nahezu keine Veränderungen an den Anwendungsprogrammen erforderlich sind und auch Sicherungskopien der Datenbank geschützt werden. Wenig sinnvoll ist es, dem MSP diese Aufgabe zu übertragen (siehe Seite 73).

Mit Blick auf die empfohlene Anbieterkennzeichnung (siehe Seite 77 f) ist es erforderlich, dass eine Verlin-

kungsmöglichkeit auf ein Impressum geschaffen wird, das stets mittels maximal 2 Klicks im Webportal erreichbar ist. Ggf. muss dies auch für eine Datenschutzerklärung erfolgen.

Auch im Kaseya Agent sollte die Möglichkeit eröffnet werden, eine Datenschutzerklärung ständig verfügbar zu halten. Unter „About Agent" sind derzeit nur Links zum Hersteller angegeben. Diese sollten editierbar sein und mit Links zu entsprechenden Informationen des MSP versehen werden können.

Datenfelder, die auf besondere personenbezogene Daten verweisen (wie etwa Krankheitsdaten (siehe dazu Seite 41 f)), werden zwar offensichtlich nicht verwendet, sollten aber aus den Datenbeständen entfernt werden, damit hier kein falscher Eindruck aufkommt.

Standardeinstellungen, die den Datenschutz betreffen, sollten möglichst restriktiv gesetzt werden. Vorschläge dazu finden sich weiter oben (siehe Seite 79 f).

Schließlich sollte überlegt werden, ob die Zugangskontrolle zum Kaseya Webportal so ergänzt werden kann, dass externe Authentifizierungssysteme eingebunden werden können.

PRODUKTDOKUMENTATION

Die Bereitstellung von Musterverträgen (Inhalte siehe Seite 84 f), Musterverfahrensbeschreibungen (Inhalte siehe Anhang A), Mustereinwilligungen (Inhalte siehe Anhänge C und D) und Musterdatenschutzerklärungen (Inhalte siehe Anhänge E und F) in der Produktdokumentation wäre ein Instrument, das den datenschutzkonformen Einsatz des *Kaseya IT Automation Framework* enorm fördern würde.

DATENSCHUTZKONFORME INSTALLATION UND KONFIGURATION

ALLGEMEINE EMPFEHLUNGEN

Aus Gründen der Transparenz wird generell empfohlen, dass die Piktogramme, die (meist) in der Systemablage eines ferngewarteten Rechners anzeigen, welche Anwendungen ausgeführt werden, nicht durch entsprechende Setzungen bei der Installation oder Konfiguration von Komponenten des *Kaseya IT Automation Framework* ausgeblendet werden.

Der Person, die einen ferngewarteten Rechner benutzt, sollten - ebenfalls aus Transparenzgründen - generell für alle installierten Anwendungen soweit Administratorrechte eingeräumt werden, dass er sich jederzeit über Details einer Anwendung informieren kann und diese ggf. beenden kann. Diese Beendigungsmöglichkeit sorgt auch dafür, dass ein Widerspruch gegen eine weitere Erhebung und Verwendung von Daten zeitnah durchgesetzt werden kann.

In den folgenden Abschnitten werden anhand von Screenshots weitere empfohlene Einstellungen verdeutlicht. Rote Hervorhebungen zeigen dabei wesentliche Aspekte.

EMPFEHLUNGEN ZU KASEYA AGENT

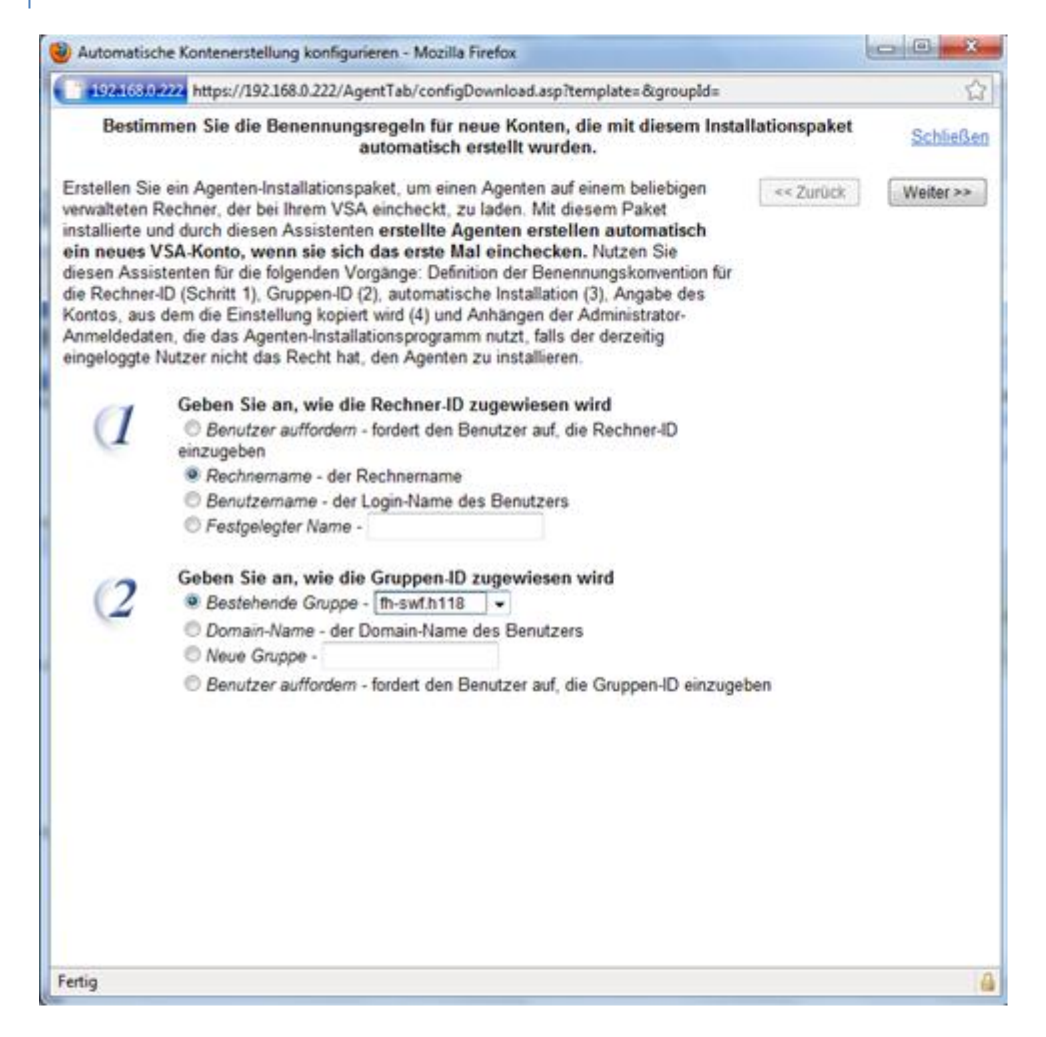


Abbildung 9: Installationspaket Teil 1

Mit der oben gezeigten Einstellung werden Agenten mit ihrem Rechnernamen in der Abteilung **h118** der Organisation **fh-swf** angelegt.

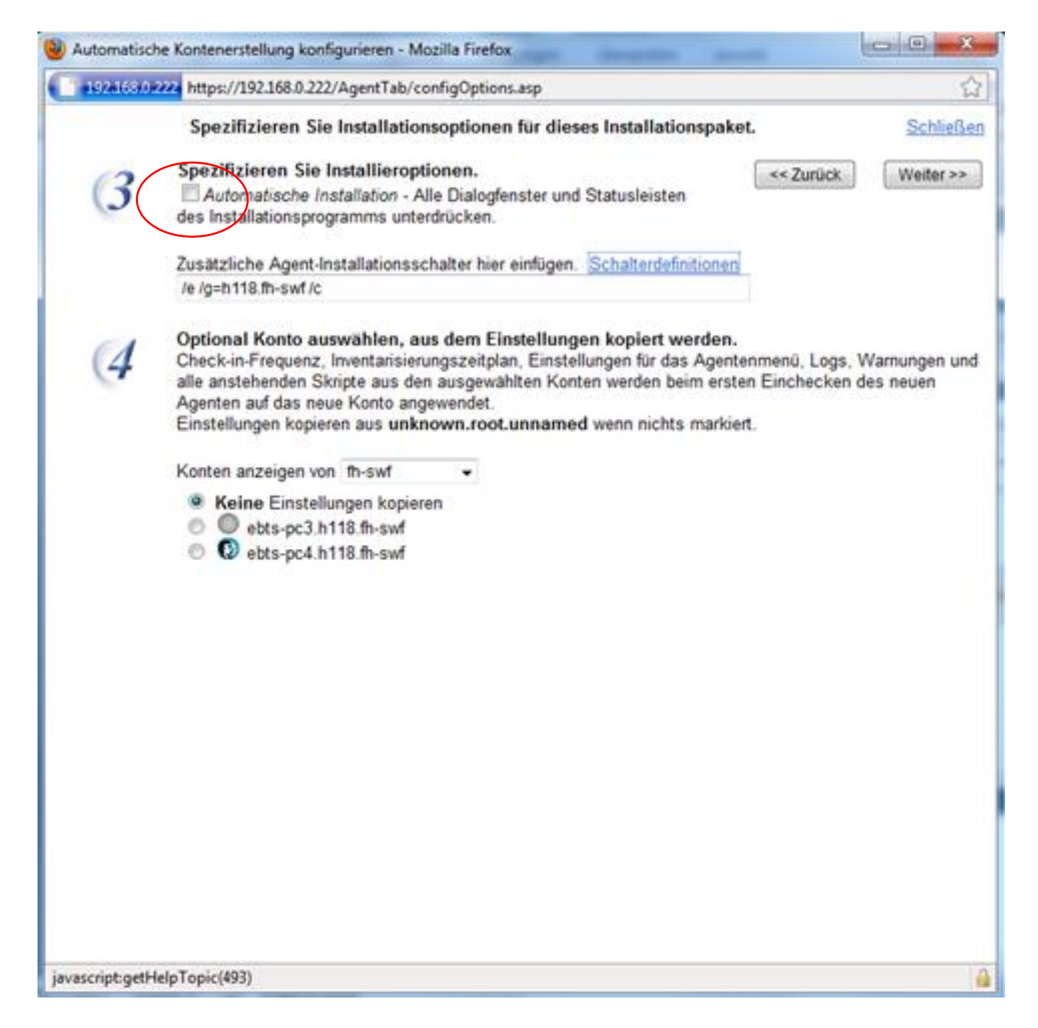


Abbildung 10: Installationspaket Teil 2

Die Agenteninstallation wird voll transparent für den Benutzer des fernzuwartenden Rechners vorgenommen.

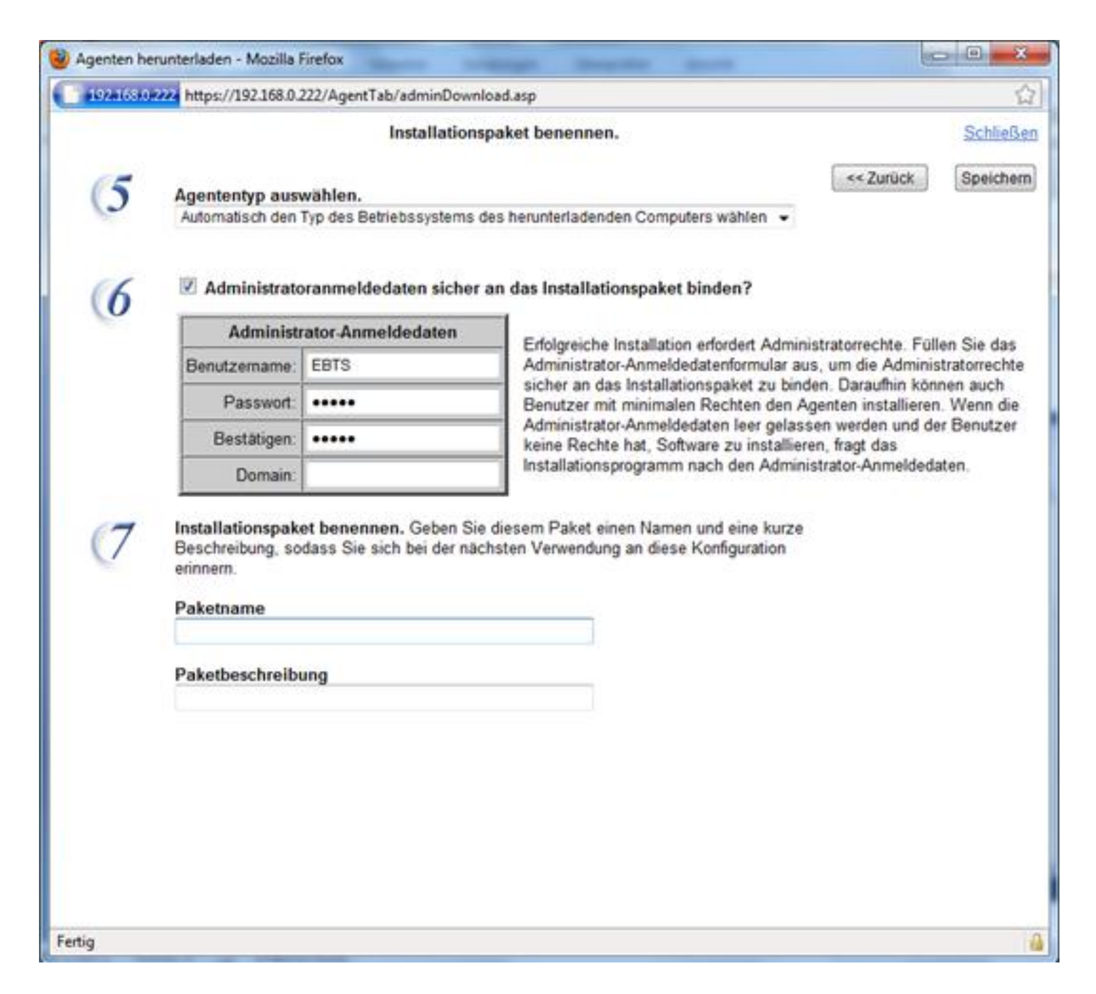


Abbildung 11: Installationspaket Teil 3

Auch Benutzer ohne Administratorrechte können mit der oben gezeigten Einstellung das Installationspaket verwenden.

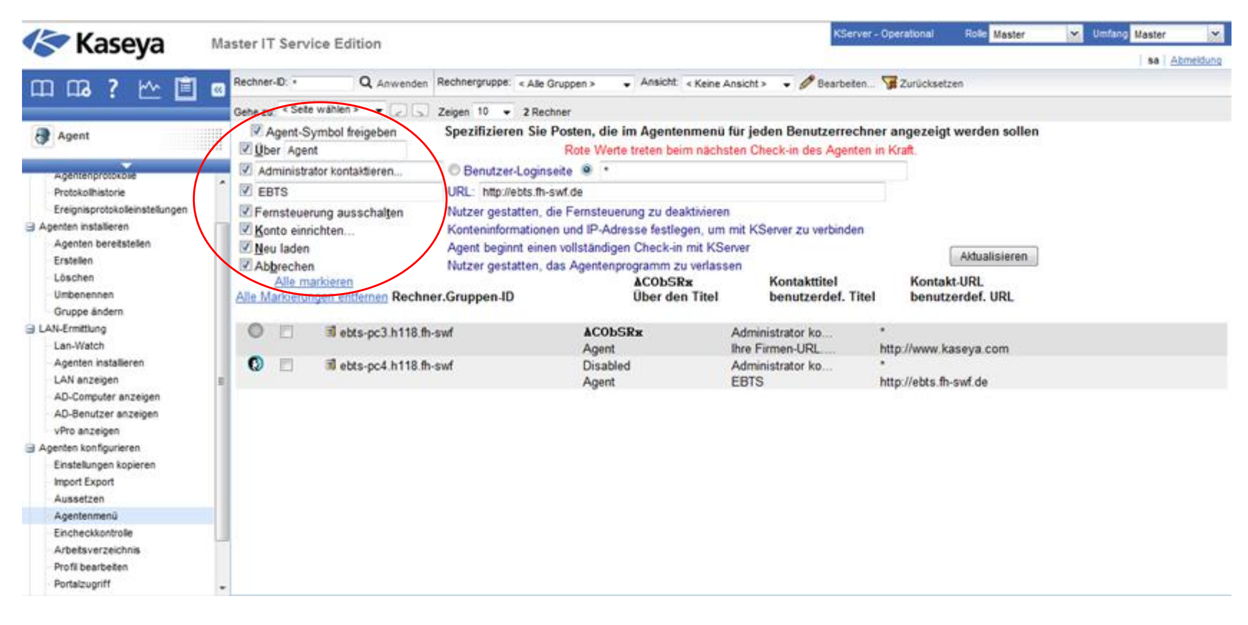


Abbildung 12: Konfiguration der Agentenmenüs

Nach der Installation muss das Agentenmenü - wie oben gezeigt - angepasst werden.

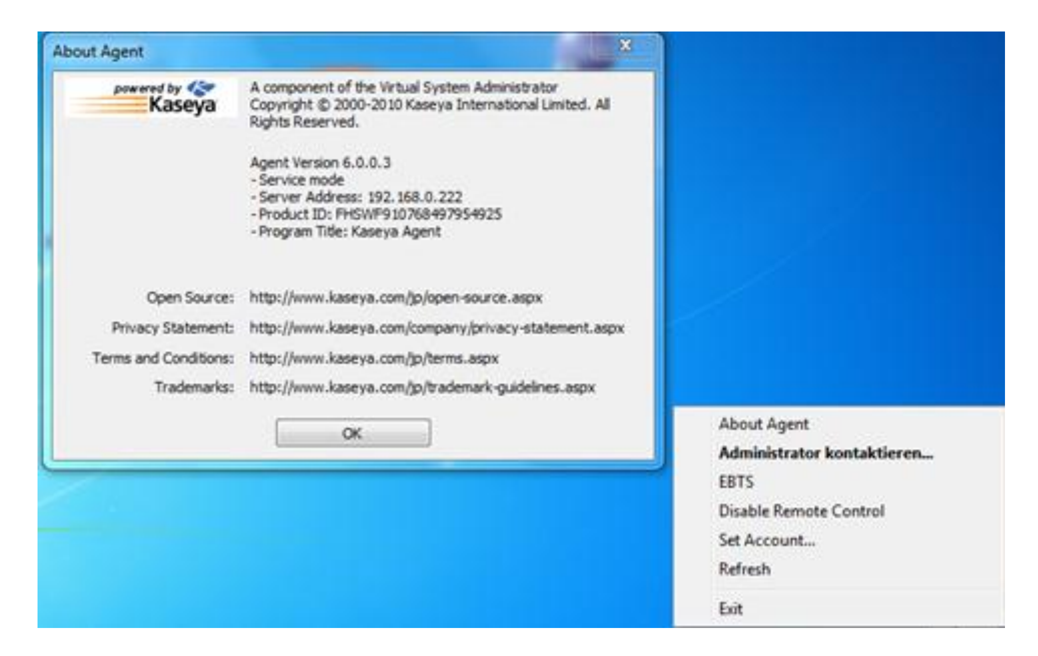


Abbildung 13: Agentenmenü und 'About Agent'

Danach bietet sich auf dem ferngewarteten Rechner obiges Bild. In ‚About Agent' gibt es zwar Links zu einer Datenschutzerklärung und weiteren Informationen. Diese können aber (noch) nicht angepasst werden.

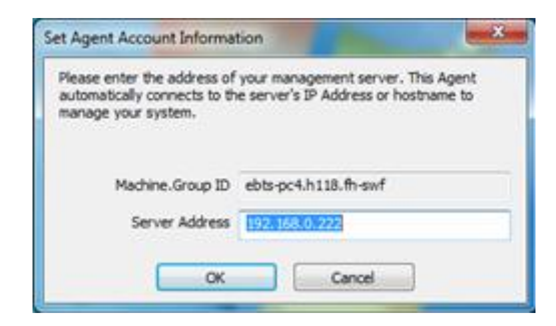


Abbildung 14: Set Account …

Der Menüpunkt ‚Set Account…' erlaubt die (temporäre) Änderung der Server-IP-Adresse.

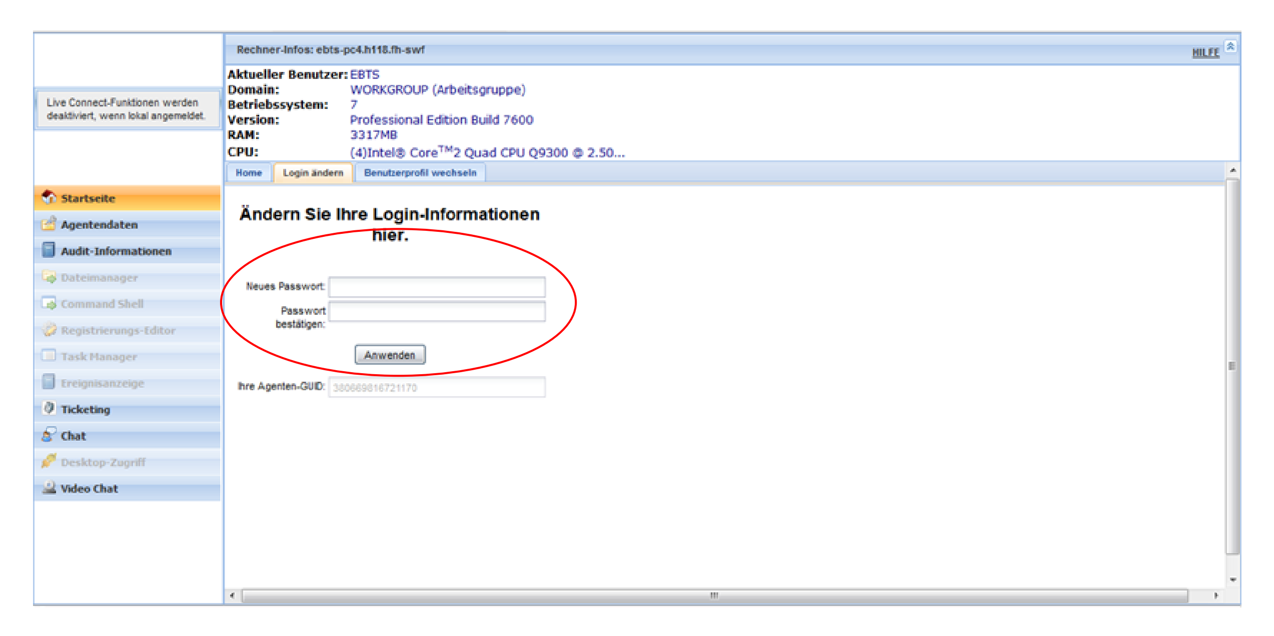


Abbildung 15: Agenten Login Teil 1

Durch Klicken auf das Kaseya Piktogramm kann der Benutzer des ferngewarteten Rechners eine Verbindung zum Kaseya Server und Webportal herstellen. Dabei kann er (wenn – wie empfohlen - freigeschaltet) sein Benutzerkennwort ändern.

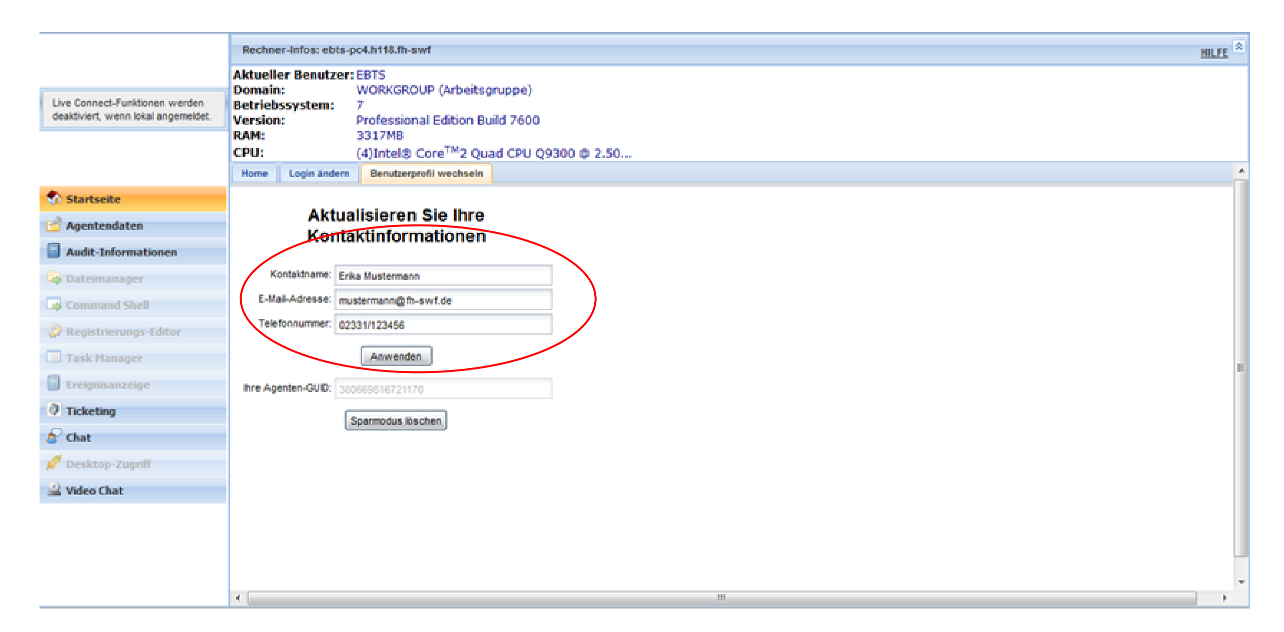


Abbildung 16: Agenten Login Teil 2

Zusätzlich kann der Benutzer des ferngewarteten Rechners wesentliche personenbezogene Daten ändern oder löschen (wenn – wie empfohlen - freigeschaltet).

EMPFEHLUNGEN ZU KASEYA SERVER UND WEBPORTAL



Abbildung 17: Bearbeitungsmöglichkeiten der Anmeldeseite

Wie obige Abbildung zeigt, lassen sich weder Datenschutzerklärung noch Impressum derzeit in der Anmeldeseite des Webportals verändern.

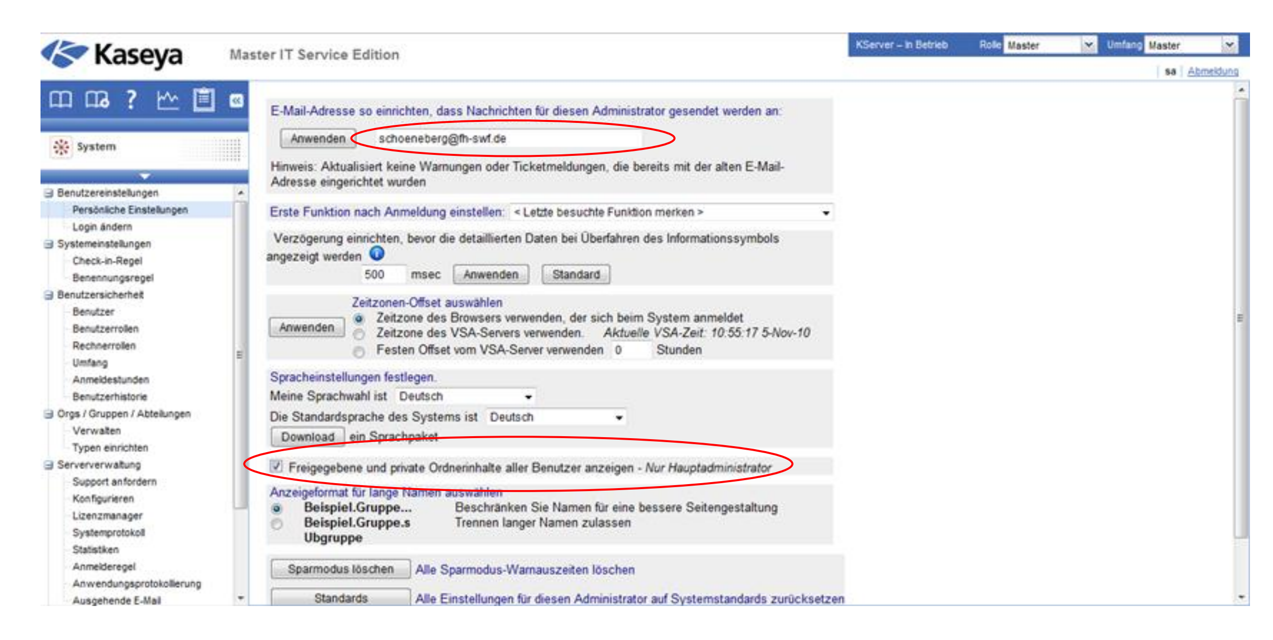


Abbildung 18: Allgemeine Einstellungen des Servers

Falls Bedenken bestehen, kann dem Systemadministrator (hier Hauptadministrator genannt) der Zugriff auf die Ordnerinhalte anderer Benutzer entzogen werden. Dies kann allerdings die Administration wesentlich erschwe-

ren.

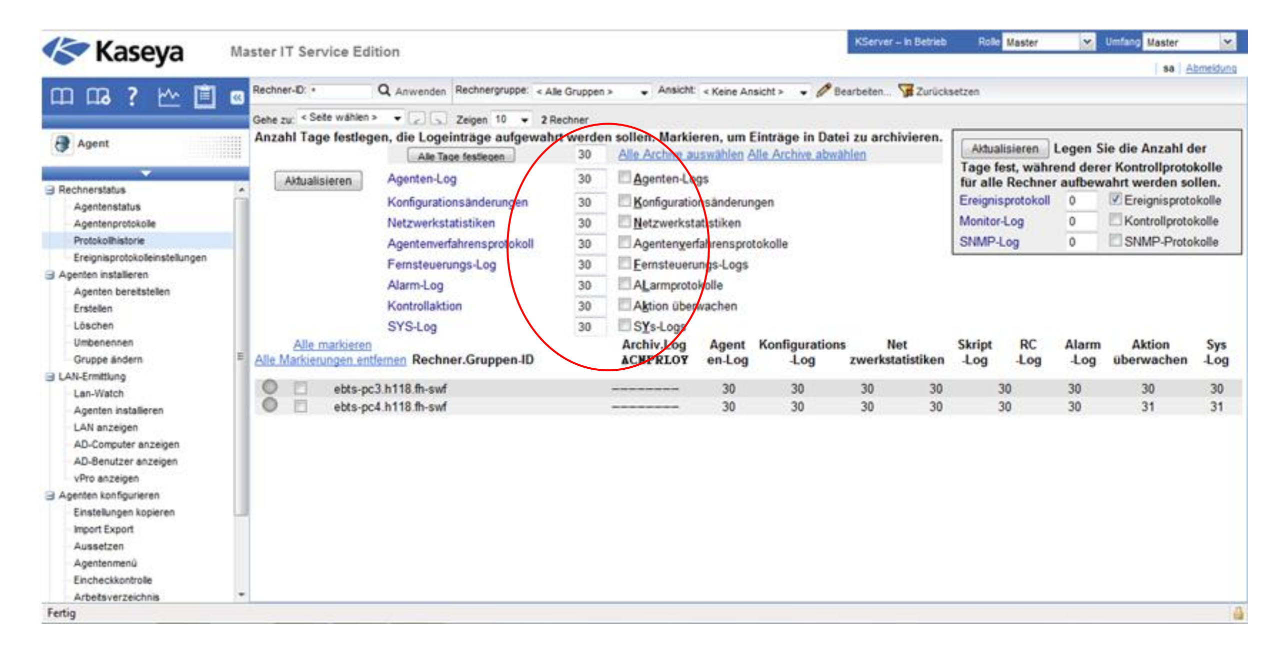


Abbildung 19: Protokoll- und Logeinstellungen

Ohne individuelle Begründungen für anders lautende Festlegungen ist der obige Vorschlag zu Aufbewahrungszeiten und Archivierungen ein guter Ausgangspunkt.

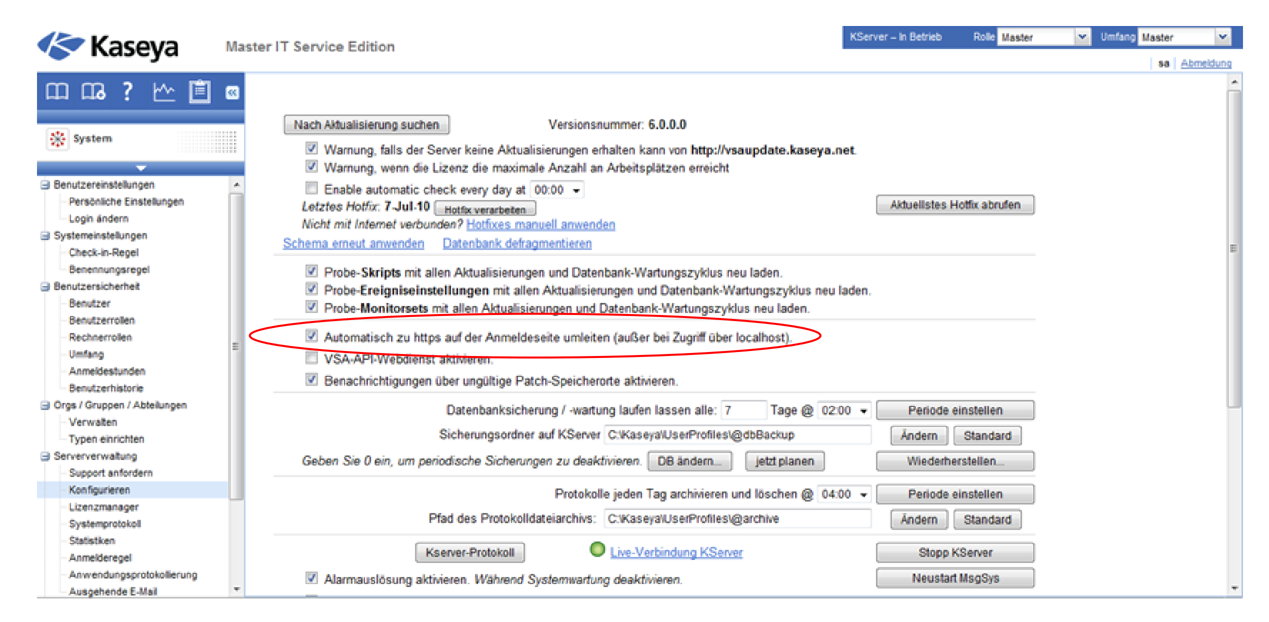


Abbildung 20: Konfiguration des Protokolls

Ein Zugriff auf das Webportal sollte nur über das HTTPS-Protokoll erfolgen können.

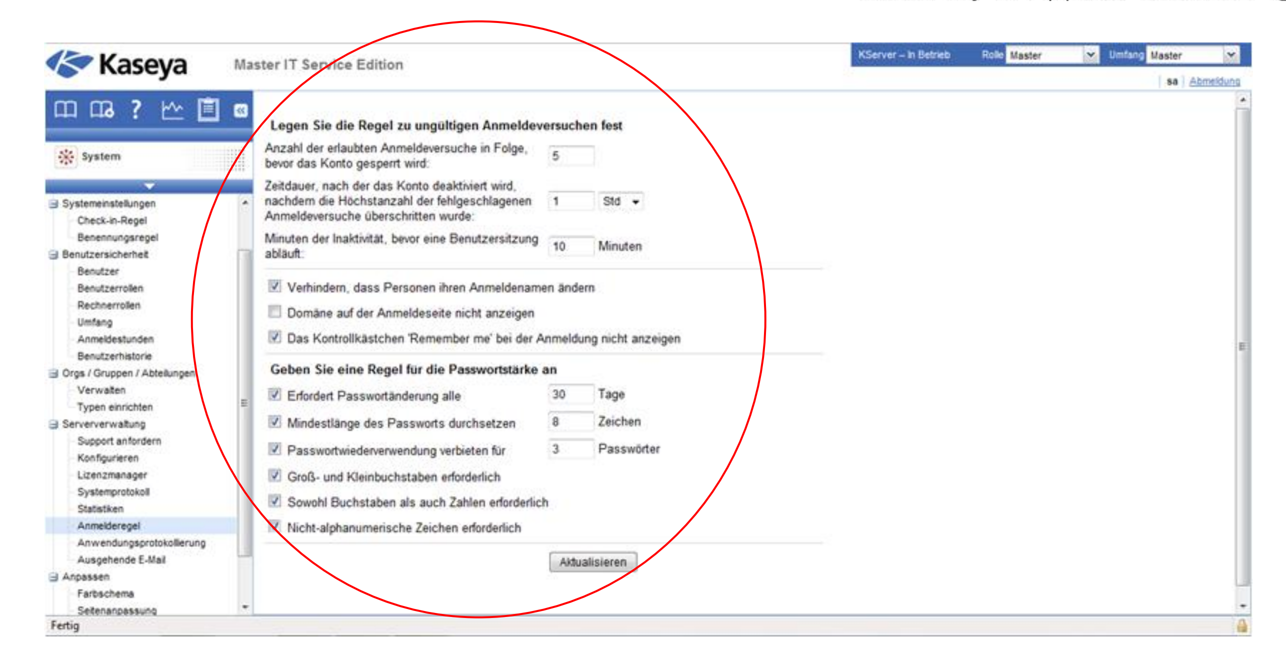


Abbildung 21: Allgemeine Anmelderegeln

Auf dieser Seite muss neben den Authentikationsparametern auch konfiguriert werden, ob der Benutzername auf dem lokalen Rechner gespeichert wird. Dies wird nicht empfohlen.

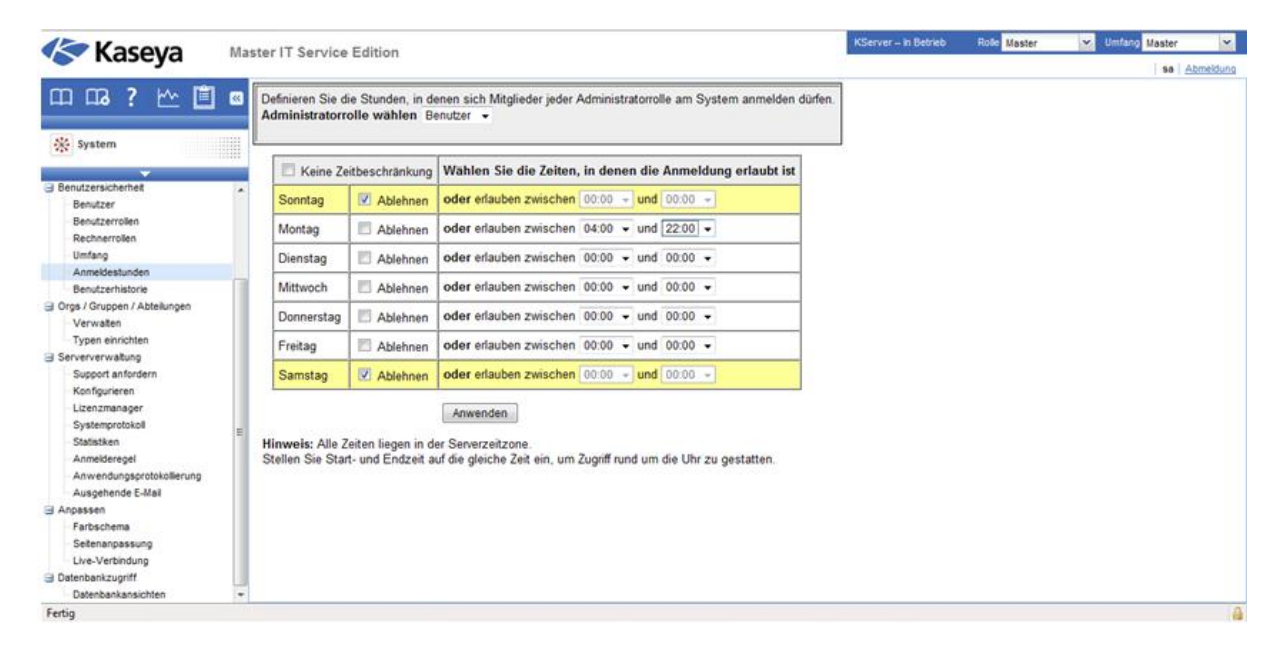


Abbildung 22: Rollenbezogene Anmeldestunden

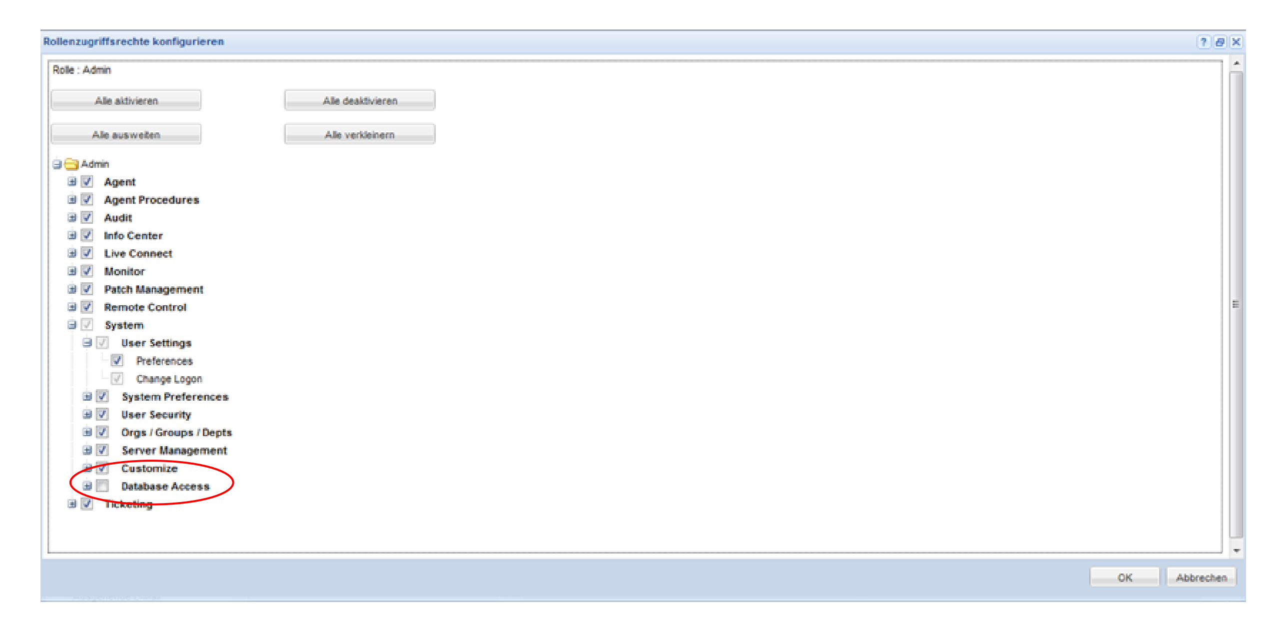


Abbildung 23: Benutzerbezogene Zugriffsrechte

Hier ist wichtig, dass der direkte Zugriff auf die Datenbank generell ausgeschlossen wird.

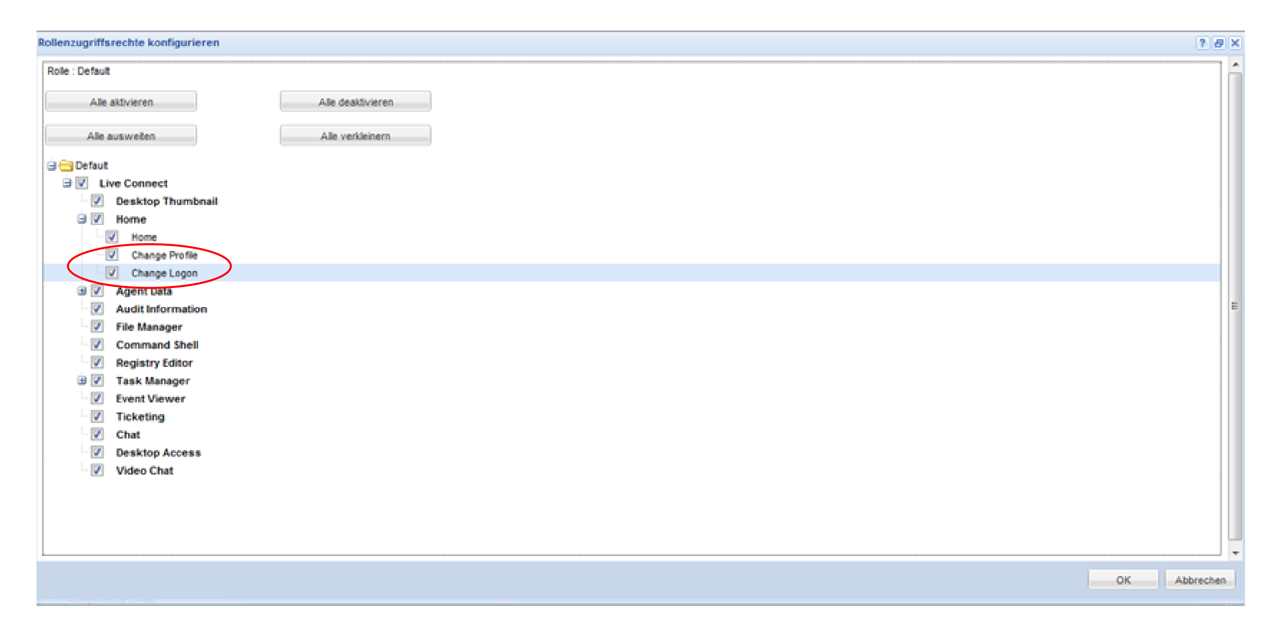


Abbildung 24: Rechnerbezogene Zugriffsrechte

Sowohl Login- als auch Kontaktinformationen sollten durch den Benutzer editierbar sein.



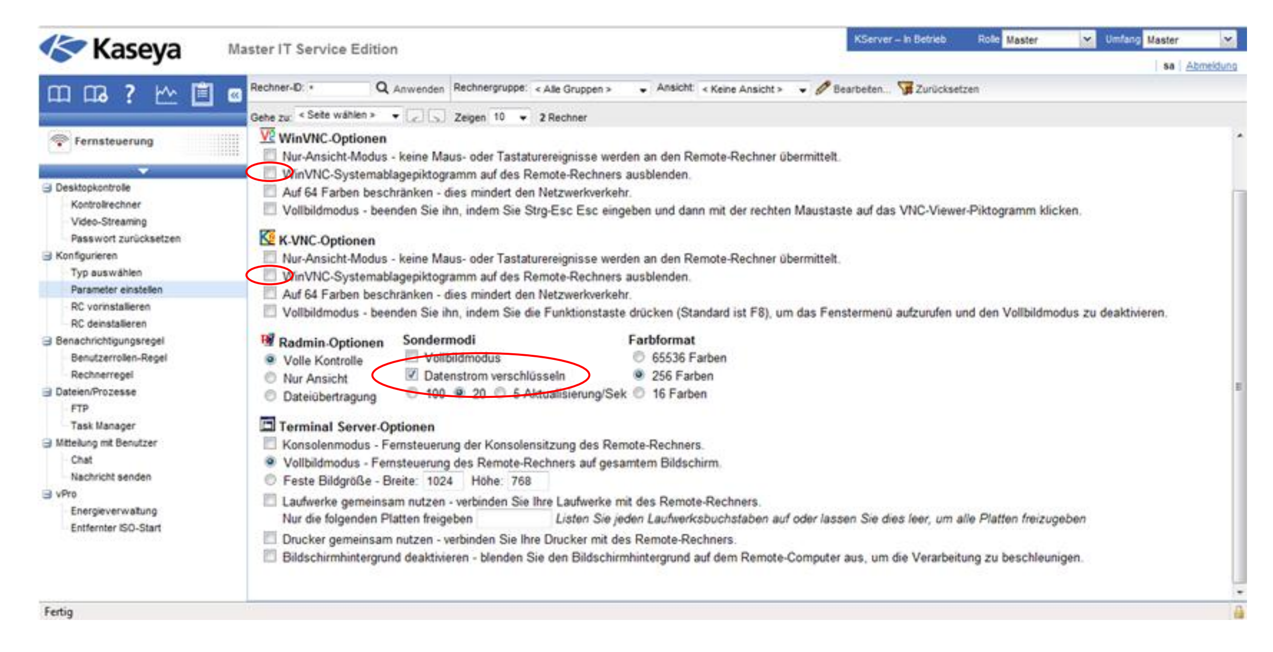


Abbildung 25: Konfiguration Fernzugriffe

Für **Radmin** muss die Verschlüsselung explizit aktiviert werden. Piktogramme sollten auf den ferngewarteten Rechnern nicht ausgeblendet werden.



ANHANG A: BEISPIEL EINER VERFAHRENSBESCHREIBUNG ENTSPRECHEND § 4E BDSG

Meldeformular zur

automatisierten Verarbeitung nach § 4e BDSG

(bitte an den Datenschutzbeauftragten übersenden)

Nur auszufüllen, wenn **personenbezogenen Daten verwendet werden!**

Anmerkung: Soweit der Platz dieses Formulars nicht ausreicht fügen Sie bitte zusätzliche Anlagen bei.

Projekt-Nr.:	☐	**Änderung bestehendes Verfahren**	☐	**Eigenentwickelte Software**
Ggf. Einführungstermin:	x	**Neues Verfahren**	x	**Standard- bzw. Kauf-Software**

1. Grundsätzliche Angaben zum Verfahren und zur Verantwortlichkeit.

1.1	Bezeichnung und genaue Beschreibung des Verfahrens: Automatisiertes Verfahren zur Fernwartung und Fernbetreuung von IT-Infrastrukturen auf Basis des *Kaseya IT Automation Framework*.		
1.2	Fachbereich: Abteilung Personal	Verantwortliche Führungskraft: Herr Leitermann	ggf.: Stellen-Kennzeichen: 123
1.3	Ausfüllende Person: Rainald Schöneberg		Telefon-Nummer: 987654321
1.4	Name u. Anschrift des Auftragnehmers, wenn Auftragsdaten-verarbeitung nach § 11 BDSG: Musterfirma, Musterstr. 123, 12345 Musterstadt		Vertrags-Nummer: V12345

2. Zweckbestimmung und Rechtsgrundlage der Datenverarbeitung

2.1	Fernwartung der Abteilungsrechner (Hardware und Microsoft-Betriebssysteme) einschließlich Patch-Management von Microsoft-Office. Fernbetreuung der Benutzer der Abteilungsrechner.	
2.2	Rechtsgrundlage bitte ankreuzen soweit zutreffend und erläutern	
	☐ Vertrag oder Vertragsanbahnung mit dem Betroffenen	
	x Einwilligung des Betroffenen	☐ Vorrangige Rechtsvorschriften
	☐ Interessenabwägung	x Sonstiges (bitte erläutern)
	Erläuterung: Entsprechende Dienst- und Betriebsvereinbarungen.	

3. a Art der gespeicherten Daten/ Datenkategorien	Kreis der betroffenen Personengruppen
Angaben zur Person (Vor- und Nachname, Telefon, Email)	Angestellte Mitarbeiter
Zugangsdaten (Benutzerkennung, Benutzerkennwort)	
Technische Daten (Inventar, Ereignisse, Alarme)	
Protokolldaten (Rechnernutzung, Konfigurationsänderungen)	
Service-Desk-Daten (Aufträge, Lösungen)	
Sonstiges (Übertragene Dateien, Backup-Dateien)	

3. b	**Welche besonderen Arten von Daten werden verarbeitet?**
	☐ Daten zur Gesundheit
	☐ Daten zum Sexualleben
	☐ Daten über rassische und ethnische Herkunft
	☐ Daten zu politischen Meinungen
	☐ Daten zu religiösen oder philosophischen Überzeugungen



	☐ Daten zur Gewerkschaftszugehörigkeit	
	x Keine dieser Daten	
	Rechtsgrundlage für diese besonderen Daten (bitte ankreuzen soweit zutreffend)	
	☐ Vertrag oder Vertragsanbahnung mit dem Betroffenen	
	☐ Einwilligung des Betroffenen	☐ Vorrangige Rechtsvorschriften
	☐ Interessenabwägung	☐ Sonstiges (bitte erläutern)
	Erläuterungen	

4. Art übermittelter Daten und deren Empfänger

Interne Empfänger (innerhalb derselben juristischen Person)

Interne Stelle (Org-Einheit)	Art der Daten	Zweck der Daten-Mitteilung
IT-Administration	Angaben zur Person, Zugangsdaten	Administration, Dokumentation
Geschäftsleitung	Statistiken auf Basis der technischen Daten, der Protokolldaten und der Service-Desk-Daten	Prüfung der IT-Infrastruktur und der Vertragserfüllung

Externe Empfänger und Dritte (jeder andere Empfänger, auch Konzernunternehmen)

Externe Stelle	Art der Daten	Zweck der Daten-Mitteilung
Musterfirma	Alle	Fernwartung/Fernbetreuung

Geplante Datenübermittlung in Drittstaaten (außerhalb der EU)

Welcher Staat	Art der Daten	Zweck der Daten-Mitteilung

5. Regelfristen für die Löschung der Daten

30 Tage oder entsprechend gesetzlicher Bestimmungen

Ist eine fristabhängige Löschung vorgesehen?

x Ja ☐ Nein

6. Zugriffsberechtigte Personengruppen (Berechtigungsgruppen)

Administratoren der Musterfirma
Geschäftsleitung

Die Berechtigungen werden über das Berechtigungsverfahren in SAP administriert.

☐ Ja ☐ Nein

Die Berechtigungen werden über ein eigenes Berechtigungsverfahren in der Anwendung administriert.

x Ja ☐ Nein

7. Technische und organisatorische Maßnahmen (§ 9 BDSG)	
Hinsichtlich der Datensicherheitsmaßnahmen wurde der Bereich IT-Sicherheit eingebunden x Ja ☐ Nein	
Die Maßnahmen entsprechen dem allgemeinen IT-Sicherheitskonzept des Unternehmens? ☐ Ja x Nein	
Falls Nein, bitte Angaben zu den folgenden Maßnahmen ergänzen:	**Termin**
Zutrittskontrolle:	
Zugangskontrolle: Verschärfung der Regeln zur Benutzerkennwortkomplexität	31.12.2010
Zugriffskontrolle: Rollenmodelle in Verbindung mit Umfangsdefinitionen	31.12.2010
Weitergabekontrolle: Nutzung des HTTPS-Protokolls	31.12.2010
Eingangskontrolle:	
Auftragskontrolle:	
Verfügbarkeitskontrolle: Nutzung von dedizierter Hardware	30.06.2011
Zweckbindungsgebot:	



ANHANG B: BEISPIEL EINER EINWILLIGUNG FÜR DEN EINSATZ DES KASEYA IT AUTOMATION FRAMEWORK AUF EINEM FERNGEWARTETEN RECHNER

Wir beabsichtigen, durch einen Dienstleister ein automatisiertes Verfahren zur Fernwartung und Fernbetreuung von IT-Infrastrukturen auf Basis des *Kaseya IT Automation Framework* einzusetzen. Dazu ist es erforderlich, auf Ihrem Rechner Software zu installieren, die Informationen über Ihren Rechner an einen Server übermitteln kann und die Aufgaben, die durch den Dienstleister bestimmt werden, ausführen kann.

Dazu wollen wir dem Dienstleister Ihren Vor- und Nachnamen, Ihre Email-Adresse, Ihre Telefonnummer und Ihre Anmeldedaten (Benutzerkennung, Benutzerkennwort) für Ihren Rechner weitergeben.

Der Dienstleister wird dann die erforderliche Software auf Ihrem Rechner installieren und betreiben. Diese Software erfasst und überträgt folgende Daten, die Bezüge zu Ihrer Person haben können:

- Technische Daten: Inventar, Ereignisse, Alarme
- Protokolldaten: Rechnernutzung, Konfigurationsänderungen
- Service-Desk-Daten: Aufträge, Lösungen
- Sonstiges: Übertragene Dateien, Backup-Dateien

Der Dienstleister verpflichtet sich, beim Einsatz dieses automatisierten Verfahrens die gesetzlichen Datenschutzbestimmungen einzuhalten, insbesondere das Bundesdatenschutzgesetz (BDSG) zu beachten, um hinreichenden Schutz Ihrer oben genannten personenbezogenen Daten zu erreichen. Er verpflichtet sich zudem, keine Einsicht in Daten zu nehmen, deren Kenntnis zur Erledigung seiner Aufgaben nicht erforderlich ist.

Die oben genannten personenbezogenen Daten werden für den Zweck der Fernwartung Ihres Rechners und für die Fernbetreuung Ihrer Person erhoben oder verwendet. Eine weitergehende Verwendung der Daten erfolgt nur anonym und nur für statistische Zwecke. Insbesondere werden diese Daten nicht für eine Beurteilung Ihrer Leistung oder Ihres Verhaltens herangezogen.

Mit Ihrer Unterschrift gestatten Sie die Erhebung und die Verwendung der oben genannten personenbezogenen Daten für diesen Zweck.

Die Verweigerung der Einwilligung hat zur Folge, dass eine Fernwartung Ihres Rechners und eine Fernbetreuung Ihrer Person zunächst nicht erfolgen können.

Sie können jederzeit eine erteilte Einwilligung mit Wirkung für die Zukunft auf Dauer widerrufen. Zudem können Sie jederzeit temporär die auf Ihrem Rechner zur Fernwartung und Fernbetreuung installierte Software deaktivieren.



ANHANG C: BEISPIEL EINER EINWILLIGUNG FÜR DIE NUTZUNG DES WEBPORTALS DES KASEYA IT AUTOMATION FRAMEWORK

Durch Vergabe einer Benutzerkennung und eines Benutzerkennworts erhalten Sie Zugang zum Webportal des *Kaseya IT Automation Framework*.

Für die Einrichtung dieses Zugangs erheben wir Ihren Vor- und Nachnamen und Ihre Email-Adresse.

Diese Daten verwenden wir ausschließlich für Kommunikationsvorgänge im Rahmen der Fernwartung und Fernbetreuung auf Basis des *Kaseya IT Automation Framework*.

Bei Ihrer Nutzung unseres Webportals werden zudem folgende Daten zu Ihrer Person automatisch erfasst und gespeichert:

- die von Ihnen aufgerufenen Funktionen mit Datum, Uhrzeit und ggf. Eingabedaten,
- der von Ihnen verwendete Browser und
- Ihre IP-Adresse.

Diese Daten speichern wir zur Sicherstellung der Revisionsfähigkeit des *Kaseya IT Automation Framework*. Zusätzlich werten wir diese Daten anonym und zu statistischen Zwecken aus, um unser Webportal zu verbessern. Eine Auswertung hinsichtlich einer Überwachung oder Bewertung Ihres Arbeitsverhaltens findet nicht statt.

Sofern Sie Leistungen im Webportal anfordern, werden weitere Daten zu Ihrer Person erhoben. Diese von Ihnen freiwillig zur Verfügung gestellten personenbezogenen Daten verwenden wir ohne Ihre gesonderte Einwilligung ausschließlich nur, um die von Ihnen angeforderten Leistungen zu erbringen. Im Rahmen der Leistungserbringung können Ihre personenbezogenen Daten von uns jedoch an Dritte weitergegeben werden, sofern dies zur Leistungserbringung notwendig ist. Dritte sind z.B. Lieferanten oder Versanddienstleister, die mit dem Transport einer Ware beauftragt werden.

Mit Ihrer Unterschrift gestatten Sie die Erhebung und die Verwendung der oben genannten personenbezogenen Daten mit den genannten Beschränkungen.

Die Verweigerung der Einwilligung hat zur Folge, dass ein Zugang zum Webportal zunächst für Sie nicht eingerichtet werden kann.

Sie können jederzeit eine erteilte Einwilligung mit Wirkung für die Zukunft widerrufen.



ANHANG D: BEISPIEL EINER DATENSCHUTZERKLÄRUNG (KASEYA WEBPORTAL)

Der Schutz Ihrer Privatsphäre ist unser Anliegen

Wir möchten, dass Sie sich bei der Nutzung des Webportals des *Kaseya IT Automation Framework* auch hinsichtlich des Schutzes Ihrer personenbezogenen Daten sicher fühlen.

Unsere Mitarbeiter sind von uns zur Verschwiegenheit und zur Einhaltung der Bestimmungen des Bundesdatenschutzgesetzes verpflichtet.

Unsere technischen und organisatorischen Maßnahmen zum Schutz Ihrer personenbezogenen Daten entsprechen voll umfänglich dem Stand der Technik.

Nach dem Bundesdatenschutzgesetz haben Sie ein Recht auf unentgeltliche Auskunft über Ihre gespeicherten Daten sowie ggf. ein Recht auf Berichtigung, Sperrung oder Löschung dieser Daten.

Wir möchten Sie darauf hinweisen, dass Sie Ihre an uns gegebene Einwilligung zur Nutzung des Webportals jederzeit mit Wirkung für die Zukunft widerrufen können.

Personenbezogene Daten

Personenbezogene Daten sind Informationen zu Ihnen, zu den von Ihnen gewünschten Leistungen und zu Ihrer Nutzung dieses Webportals.

Mit der Anmeldung an unserem Webportal sind uns Ihr Vor- und Zuname sowie Ihre Email-Adresse bereits bekannt. Diese Daten verwenden wir ausschließlich für Kommunikationsvorgänge im Rahmen der Fernwartung und Fernbetreuung auf Basis des *Kaseya IT Automation Framework*.

Wir erheben und verwenden darüber hinaus nur:

- Personenbezogene Daten, die Sie uns freiwillig zur Verfügung stellen (z.B. in einer Schulungsanforderung oder in einer Fehlermeldung), sowie
- Personenbezogene Daten, die wir automatisch bei Ihrer Nutzung des Webportals erfassen können (z.B. die von Ihnen ausgeführte Funktion oder die von Ihnen veranlasste Änderung einer Konfiguration jeweils mit Zeitstempel).

Eine Übermittlung dieser Daten an auskunftsberechtigte staatliche Institutionen und Behörden erfolgt nur im Rahmen der einschlägigen Gesetze bzw. sofern wir durch eine gerichtliche Entscheidung dazu verpflichtet sind.

Eine Weitergabe dieser Daten an sonstige Dritte erfolgt nicht ohne Ihre ausdrückliche Einwilligung.

Personenbezogene Daten, die Sie freiwillig zur Verfügung stellen

Sofern Sie Leistungen anfordern, werden zusätzlich nur solche Daten zu Ihrer Person erhoben, die wir zur Erbringung der Leistungen benötigen. Die von Ihnen freiwillig zur Verfügung gestellten personenbezogenen Daten verwenden wir ohne Ihre gesonderte Einwilligung ausschließlich, um die von Ihnen angeforderten Leistungen zu erbringen. Im Rahmen der Leistungserbringung können Ihre personenbezogenen Daten von uns an Dritte weitergegeben werden, sofern dies zur Leistungserbringung notwendig ist. Dritte sind z.B. Lieferanten oder Versanddienstleister, die mit dem Transport einer Ware beauftragt werden.

Personenbezogene Daten, die automatisch bei der Nutzung des Webportals erfasst werden

Bei Ihrer Nutzung unseres Webportals werden folgende Daten zu Ihrer Person automatisch erfasst und gespeichert:

- die von Ihnen aufgerufenen Funktionen mit Datum, Uhrzeit und ggf. Eingabedaten,
- der von Ihnen verwendete Browser und
- Ihre IP-Adresse.

Diese Daten speichern wir zur Sicherstellung der Revisionsfähigkeit des *Kaseya IT Automation Framework*.

Zusätzlich werten wir diese Daten lediglich anonym und zu statistischen Zwecken aus, um unser Webportal zu verbessern. Eine Auswertung hinsichtlich einer Überwachung oder Bewertung Ihres Arbeitsverhaltens findet nicht statt.

Cookies

Wenn Sie unser Webportal nutzen, kann es sein, dass wir Informationen in Form eines Cookies auf Ihrem Rechner ablegen. Cookies sind kleine Text-Dateien, die von unserem Webserver an Ihren Browser gesendet und auf der Festplatte Ihres Rechners gespeichert werden.

Cookies erlauben es uns beispielsweise, das Webportal Ihren Interessen anzupassen oder Ihren Benutzernamen zu speichern, damit Sie ihn nicht jedes Mal neu eingeben müssen.

Wenn Sie die Verwendung von Cookies verhindern möchten, können Sie eine entsprechende Sperrung in Ihrem Webbrowser konfigurieren. Diese Sperrung kann sich auf einzelne Funktionen dieses Webportals auswirken.

Sicherheit

Wir treffen alle notwendigen, technischen und organisatorischen Sicherheitsmaßnahmen, um Ihre personenbezogenen Daten vor Verlust und Missbrauch zu schützen. So werden Ihre Daten in einer sicheren Betriebsumgebung gespeichert, die der Öffentlichkeit nicht zugänglich ist. Ihre personenbezogenen Daten werden bei der Übermittlung durch die sog. Secure Socket Layer-Technologie (SSL) verschlüsselt. Dies bedeutet, dass die Kommunikation zwischen Ihrem Computer und unseren Servern unter Einsatz eines anerkannten Verschlüsselungsverfahrens erfolgt, wenn Ihr Browser SSL unterstützt.

Änderung unserer Datenschutzerklärung

Der Umgang mit personenbezogenen Daten wird von uns laufend vor dem Hintergrund der datenschutzrechtlichen Bestimmungen überwacht und ggf. angepasst. Bitte nehmen Sie in regelmäßigen Abständen Kenntnis von unserer Datenschutzerklärung, die den jeweils aktuellen Stand unseres Umgangs mit persönlichen Informationen wiedergibt.

Fragen, Anregungen, Beschwerden

Wenn Sie Fragen zu unserer Datenschutzerklärung oder zur Verwendung Ihrer persönlichen Daten haben, können Sie sich direkt an unseren Datenschutzbeauftragten wenden. Er steht Ihnen auch im Falle von Auskunftsersuchen, Anregungen oder bei Beschwerden als Ansprechpartner zur Verfügung.



ANHANG E: BEISPIEL EINER DATENSCHUTZERKLÄRUNG (KASEYA AGENT)

Was ist der *Kaseya Agent*?

Kaseya Agent ist ein Dienst, der für die Fernwartung Ihres Rechners und für Ihre Fernbetreuung Informationen zur Verfügung stellt und der Aufgaben der Fernwartung ausführt. Zu diesen Aufgaben gehören beispielsweise Datensicherungen und Softwareaktualisierungen. *Kaseya Agent* wird für erweiterte Funktionalitäten durch gewisse Programme ergänzt, die etwa den Fernzugriff auf Ihren Rechner oder eine Dateiübertragung von/zu Ihrem Rechner gestatten.

Durch Ihre Einwilligung haben Sie die Erlaubnis erteilt, den Kaseya Agent und gewisse ergänzende Programme auf Ihrem Rechner zweckgebunden einzusetzen. Sie können diese Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen. Sie haben zusätzlich die Möglichkeit, den Einsatz von *Kaseya Agent* oder den Einsatz von ergänzenden Programmen temporär auszusetzen.

Welche Daten werden automatisch abgerufen?

Folgende Informationen können durch den *Kaseya Agent* abgerufen werden:

- Die Hardware, über die Ihr Rechner verfügt.
- Die Software, die auf Ihrem Rechner installiert ist oder installiert werden kann.
- Ihre Konfigurationseinstellungen.
- Informationen zu Ereignissen (Gerätedefekt, Virenfund, Softwarefehler, …), die bei der Nutzung Ihres Rechners eingetreten sind.

Welche Daten werden zusätzlich eingesehen oder abgerufen?

Je nach Konfiguration können durch die ergänzenden Programme faktisch alle Daten, die sich auf Ihrem Rechner befinden, eingesehen und abgerufen werden. Solch eine Einsicht oder solch ein Abruf finden jedoch nur statt, wenn es für die Fernwartung Ihres Rechners oder für Ihre Fernbetreuung unumgänglich ist. Sie müssen in der Regel sogar Ihre Zustimmung geben, bevor eine Einsicht oder ein Abruf erfolgt. In keinem Fall bleibt Ihnen eine Einsicht oder ein Abruf verborgen. Sie können unsere Bemühungen für den Datenschutz übrigens wirkungsvoll unterstützen, wenn Sie alle personenbezogenen Daten, die sich auf Ihrem Rechner befinden, gegen unbefugten Zugriff zusätzlich schützen, indem Sie etwa diese Daten sicher verschlüsseln.

Wie werden die eingesehenen oder abgerufenen Daten verwendet?

Die eingesehenen oder abgerufenen Daten werden zur Fernwartung ihres Rechners und zu Ihrer Fernbetreuung verwendet. Die Daten werden auch dazu verwendet, Statistiken zur Analyse von Trends sowie zur Verbesserung unserer Dienstleistungen zu erstellen.

Daten, die von Ihrem Rechner abgerufen werden, werden auf unserem Server in Musterstadt gespeichert und durch erfahrene Mitarbeiter verarbeitet oder genutzt.

Wie sicher sind diese Daten?

Musterfirma ist bemüht, die Sicherheit der eingesehenen oder abgerufenen Daten zu gewährleisten. Wir verwenden verschiedene Sicherheitstechnologien und -verfahren, um dazu beizutragen, diese Daten vor unbefug-

tem Zugriff oder vor Offenlegung zu schützen. Wenn beispielsweise Ihr Rechner durchsucht wird, um die auf dem Rechner installierte Software zu ermitteln, wird eine sichere Verschlüsselung bei der Übertragung der Informationen auf unseren Server verwendet.

Was sollten Sie tun, wenn Sie Fragen oder Anmerkungen haben?

Musterfirma nimmt Ihre Anmerkungen zu dieser Datenschutzerklärung gerne entgegen. Wenn Sie glauben, dass Musterfirma diese Datenschutzbestimmungen nicht erfüllt, wenden Sie sich bitte an dsb@musterfirma.de. Wir bemühen uns in wirtschaftlich vertretbarem Umfang, das Problem umgehend zu ermitteln und zu beheben.